The Race To Quantum Correction

The Race To Quantum Correction

General
- DiVincenzo's Criteria
- NISQ Era
- Quantum Computing Timeline
- Quantum Information
- Quantum Programming
- Quantum Simulation
- Qubit Physical vs. Logical
- Quantum Processors (Cloud-Based)

Theorems
- Bell's Theorem
- Eastin–Knill Theorem
- Gleason's Theorem
- Gottesman–Knill Theorem
- Holevo's Theorem
- No-Broadcasting Theorem
- No-Cloning Theorem
- No-Communication Theorem
- No-Deleting Theorem
- No-Hiding Theorem
- No-Teleportation Theorem
- PBR Theorem
- Quantum Speed Limit Theorem
- Threshold Theorem
- Solovay–Kitaev Theorem
- Purification Theorem

Quantum Communication
- Classical Capacity (Entanglement-Assisted)
- Quantum Capacity
- Entanglement Distillation
- Monogamy of Entanglement
- LOCC (Local Operations and Classical Communication)
- Quantum Channel
- Quantum Network
- Quantum Teleportation
- Quantum Gate Teleportation
- Superdense Coding

Quantum Cryptography
- Post-Quantum Cryptography
- Quantum Coin Flipping
- Quantum Money
- Quantum Key Distribution (BB84, SARG04, and Other Protocols)
- Quantum Secret Sharing

Quantum Algorithms
- Amplitude Amplification
- Bernstein–Vazirani Algorithm
- Boson Sampling
- Deutsch–Jozsa Algorithm
- Grover's Algorithm
- HHL Algorithm
- Hidden Subgroup Problem
- Quantum Annealing
- Quantum Counting
- Quantum Fourier Transform
- Quantum Optimization
- Quantum Phase Estimation
- Shor's Algorithm
- Simon's Algorithm
- VQE (Variational Quantum Eigensolver)

Quantum Complexity Theory
- BQP
- EQP
- QIP
- QMA
- PostBQP

Quantum Processor Benchmarks
- Quantum Supremacy
- Quantum Volume
- Randomized Benchmarking
- XEB (Cross-Entropy Benchmarking)
- Relaxation Times (T1, T2)

Quantum Computing Models
- Adiabatic Quantum Computation
- Continuous-Variable Quantum Information
- One-Way Quantum Computer (Cluster State)
- Quantum Circuit and Quantum Logic Gate
- Quantum Machine Learning and Quantum Neural Network
- Quantum Turing Machine
- Topological Quantum Computer

Quantum Error Correction
- Quantum Error Correction Codes (CSS, Quantum Convolutional, Stabilizer)
- Shor Code
- Bacon–Shor Code
- Steane Code
- Toric Code
- Entanglement-Assisted Codes

Physical Implementations

Quantum Optics
- Cavity QED
- Circuit QED
- Linear Optical QC
- KLM Protocol

Ultracold Atoms
- Neutral Atom QC
- Trapped-Ion QC

Spin-Based
- Kane QC
- Spin Qubit QC
- NV Center QC
- NMR QC

Superconducting
- Charge Qubit
- Flux Qubit
- Phase Qubit
- Transmon

Quantum Programming
- OpenQASM / Qiskit / IBM QX
- Quil / Forest / Rigetti
- QCS
- Cirq
- Q#
- libquantum
- Many Others...











Libretech-Systems

Nostr Npub
npub16d8gxt2z4k9e8sdpc0yyqzf5gp0np09ls4lnn630qzxzvwpl0rgq5h4rzv

https://freedomtech.unstoppable

Acknowledgment

This document was edited from Wikipedia articles.

WIKIPEDIA
The Free Encyclopedia

DiVincenzo's criteria

The **DiVincenzo criteria** are conditions necessary for constructing a quantum computer, conditions proposed in 2000 by the theoretical physicist David P. DiVincenzo,[1] as being those necessary to construct such a computer—a computer first proposed by mathematician Yuri Manin, in 1980,[2] and physicist Richard Feynman, in 1982[3]—as a means to efficiently simulate quantum systems, such as in solving the quantum many-body problem.

There have been many proposals for how to construct a quantum computer, all of which meet with varying degrees of success against the different challenges of constructing quantum devices. Some of these proposals involve using superconducting qubits, trapped ions, liquid and solid state nuclear magnetic resonance, or optical cluster states, all of which show good prospects but also have issues that prevent their practical implementation.

The DiVincenzo criteria consist of seven conditions an experimental setup must satisfy to successfully implement quantum algorithms such as Grover's search algorithm or Shor factorization. The first five conditions regard quantum computation itself. Two additional conditions regard implementing quantum communication, such as that used in quantum key distribution. One can demonstrate that DiVincenzo's criteria are satisfied by a classical computer. Comparing the ability of classical and quantum regimes to satisfy the criteria highlights both the complications that arise in dealing with quantum systems and the source of the quantum speed up.

Statement of the criteria

According to DiVincenzo's criteria, constructing a quantum computer requires that the experimental setup meet seven conditions. The first five are necessary for quantum computation:

1. A scalable physical system with well-characterized qubit
2. The ability to initialize the state of the qubits to a simple fiducial state
3. Long relevant Quantum coherence times
4. A "universal" set of quantum gates
5. A qubit-specific measurement capability

The remaining two are necessary for quantum communication:

1. The ability to interconvert stationary and flying qubits
2. The ability to faithfully transmit flying qubits between specified locations

Justification

DiVincenzo proposed his criteria after many attempts to construct a quantum computer. Below describes why these statements are important, and presents examples.

Scalability with well-characterised qubits

Most models of quantum computation require the use of qubits. Quantum mechanically, a qubit is defined as a 2-level system with some energy gap. This can sometimes be difficult to implement physically, and so we focus on a particular transition of atomic levels. Whatever the system we choose, we require that the system remain almost always in the subspace of these two levels, and in doing so we can say it is a well-characterised qubit. An example of a system that is not well characterised would be two one-electron quantum dots, with potential wells each occupied by a single electron in one well or the other, which is properly characterised as a single qubit. However, in considering a state such as $|\mathbf{00}\rangle + |\mathbf{11}\rangle$, such a system would correspond to a two-qubit state.

With today's technology, a system that has a well characterised qubit can be created, but it is a challenge to create a system that has an arbitrary number of well-characterised qubits. Currently, one of the biggest problems being faced is that we require exponentially larger experimental setups to accommodate a greater number of qubits. The quantum computer is capable of exponential speed-ups in computing classical algorithms for prime factorisation of numbers; but if this requires an exponentially large setup, then our advantage is lost. In the case of using liquid-state nuclear magnetic resonance (NMR), it was found that increased macroscopic size led to system initialisation that left computational qubits in a highly mixed state.[4] In spite of this, a computation model was found that could still use these mixed states for computation, but the more mixed these states are the weaker the induction signal corresponding to a quantum measurement is. If this signal is below the noise threshold, a solution is to increase the size of the sample to boost the signal strength; and this is the source of the non-scalability of liquid-state NMR as a means for quantum computation. One could say that as the number of computational qubits increases they become less well characterised until a threshold is reached at which they are no longer useful.

Initialising qubits to a simple fiducial state

All models of quantum and classical computation are based on performing operations on states maintained by qubits or bits and measuring and reporting a result, a procedure that is dependent on the initial state of the system. In particular, the unitarity nature of quantum mechanics makes initialisation of the qubits extremely important. In many cases, initialisation is accomplished by letting the system anneal to the ground state. This is of particular importance when you consider quantum error correction, a procedure to perform quantum processes that are robust against certain types of noise and that require a large supply of freshly initialised qubits, which places restrictions on how fast the initialisation can be.

An example of annealing is described in a 2005 paper by Petta, et al., where a Bell pair of electrons is prepared in quantum dots. This procedure relies on T_1 to anneal the system, and the paper focuses on measuring the T_2 relaxation time of the quantum-dot system and gives an idea of the timescales involved (milliseconds), which would be a fundamental roadblock, given that then the decoherence time is shorter than the initialisation time.[5] Alternate approaches (usually involving optical pumping[6]) have been developed to reduce the initialisation time and improve the fidelity of the procedure.

Long relevant coherence times

Decoherence is a problem experienced in large, macroscopic quantum computation systems. The quantum resources used by quantum computing models (superposition or entanglement) are quickly destroyed by decoherence. Long decoherence times are desired, much longer than the average gate time, so that decoherence can be combated with error correction or dynamical decoupling. In solid-state NMR using nitrogen-vacancy centers, the orbital electron experiences short decoherence times, making computations problematic; the proposed solution has been to encode the qubit in the nuclear spin of the nitrogen atom, thus increasing the decoherence time. In other systems, such as the quantum dot, issues with strong environmental effects limit the T_2 decoherence time. Systems that can be manipulated quickly (through strong interactions) tend to experience decoherence via these very same strong interactions, and so there is a trade-off between ability to implement control and increased decoherence.

A "universal" set of quantum gates

In both classical and quantum computing, the algorithms that we can compute are restricted by the number of gates we can implement. In the case of quantum computing, a universal quantum computer (a quantum Turing machine) can be constructed using a very small set of 1- and 2-qubit gates. Any experimental setup that manages to have well-characterised qubits; quick, faithful initialisation; and long decoherence times must also be capable of influencing the Hamiltonian (total energy) of the system, in order to effect coherent changes capable of implementing a universal set of gates. A perfect implementation of gates is not always necessary, as gate sequences can be created that are more robust against certain systematic and random noise models.[7] Liquid-state NMR was one of the first setups capable of implementing a universal set of gates, through the use of precise timing and magnetic field pulses. However, as mentioned above, this system was not scalable.

A qubit-specific measurement capability

For any process modifying the quantum states of qubits, the final measurement of those states is of fundamental importance when performing computations. If our system allows for non-destructive projective measurements, then, in principle, this can be used for state preparation. Measurement is at the foundation of all quantum algorithms, especially in concepts such as quantum teleportation. Measurement techniques that are not 100% efficient are typically repeated to increase the success rate. Examples of reliable measurement devices are found in optical systems where homodyne detectors have reached the point of reliably counting how many photons have passed through the detecting cross-section. More challenging is the measurement of quantum dots, where the energy gap between the $|01\rangle + |10\rangle$ and $|01\rangle - |10\rangle$ (the singlet state) is used to measure the relative spins of the two electrons.[5]

Interconverting stationary and flying qubits and faithfully transmitting flying qubits between specified locations

Interconverting and transmitting are necessary when considering quantum communication protocols, such as quantum key distribution, that involve the exchange of coherent quantum states or entangled qubits (for example, the BB84 protocol). When creating pairs of entangled qubits in experimental setups, these qubits are usually "stationary" and cannot be moved from the laboratory. If these qubits can be sent as flying qubits, such as being encoded into the polarisation of a photon, then sending entangled photons to a third party and having them extract that information, leaving two entangled stationary qubits at two different locations, can be considered. The ability to transmit the flying qubit without decoherence is a

major problem. Currently, at the Institute for Quantum Computing there are efforts to produce a pair of entangled photons and transmit one of the photons to some other part of the world by reflecting it off a satellite. The main issue now is the decoherence the photon experiences whilst interacting with particles in the atmosphere. Similarly, some attempts have been made to use optical fibres, although the attenuation of the signal has kept this from becoming a reality.

See also

- Quantum computing
- Nuclear magnetic resonance quantum computer
- Trapped ion quantum computer

References

1. DiVincenzo, David P. (2000-04-13). "The Physical Implementation of Quantum Computation". *Fortschritte der Physik*. **48** (9–11): 771–783. arXiv:quant-ph/0002077 (https://arxiv.org/abs/quant-ph/0002077). Bibcode:2000ForPh..48..771D (https://ui.adsabs.harvard.edu/abs/2000ForPh..48..771D). doi:10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E (https://doi.org/10.1002%2F1521-3978%28200009%2948%3A9%2F11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E).
2. Manin, Yu. I. (1980). *Vychislimoe i nevychislimoe* (https://web.archive.org/web/20130510173823/http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) [*Computable and Noncomputable*] (in Russian). Sov.Radio. pp. 13–15. Archived from the original (http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) on 2013-05-10. Retrieved 2013-03-04.
3. Feynman, R. P. (June 1982). "Simulating physics with computers". *International Journal of Theoretical Physics*. **21** (6): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). CiteSeerX 10.1.1.45.9310 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9310). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179).
4. Menicucci NC, Caves CM (2002). "Local realistic model for the dynamics of bulk-ensemble NMR information processing". *Physical Review Letters*. **88** (16): 167901. arXiv:quant-ph/0111152 (https://arxiv.org/abs/quant-ph/0111152). Bibcode:2002PhRvL..88p7901M (https://ui.adsabs.harvard.edu/abs/2002PhRvL..88p7901M). doi:10.1103/PhysRevLett.88.167901 (https://doi.org/10.1103%2FPhysRevLett.88.167901). PMID 11955265 (https://pubmed.ncbi.nlm.nih.gov/11955265).
5. Petta, J. R.; Johnson, A. C.; Taylor, J. M.; Laird, E. A.; Yacoby, A.; Lukin, M. D.; Marcus, C. M.; Hanson, M. P.; Gossard, A. C. (September 2005). "Coherent Manipulation of Coupled Electron Spins in Semiconductor Quantum Dots". *Science*. **309** (5744): 2180–2184. Bibcode:2005Sci...309.2180P (https://ui.adsabs.harvard.edu/abs/2005Sci...309.2180P). CiteSeerX 10.1.1.475.4833 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.475.4833). doi:10.1126/science.1116955 (https://doi.org/10.1126%2Fscience.1116955). PMID 16141370 (https://pubmed.ncbi.nlm.nih.gov/16141370).
6. Atatüre, Mete; Dreiser, Jan; Badolato, Antonio; Högele, Alexander; Karrai, Khaled; Imamoglu, Atac (April 2006). "Quantum-Dot Spin-State Preparation with Near-Unity Fidelity" (https://doi.org/10.1126%2Fscience.1126074). *Science*. **312** (5773): 551–553. Bibcode:2006Sci...312..551A (https://ui.adsabs.harvard.edu/abs/2006Sci...312..551A). doi:10.1126/science.1126074 (https://doi.org/10.1126%2Fscience.1126074). PMID 16601152 (https://pubmed.ncbi.nlm.nih.gov/16601152).

7. Green, Todd J.; Sastrawan, Jarrah; Uys, Hermann; Biercuk, Michael J. (September 2013). "Arbitrary quantum control of qubits in the presence of universal noise". *New Journal of Physics*. **15** (9): 095004. arXiv:1211.1163 (https://arxiv.org/abs/1211.1163). Bibcode:2013NJPh...15i5004G (https://ui.adsabs.harvard.edu/abs/2013NJPh...15i5004G). doi:10.1088/1367-2630/15/9/095004 (https://doi.org/10.1088%2F1367-2630%2F15%2F9%2F095004).

Retrieved from "https://en.wikipedia.org/w/index.php?title=DiVincenzo%27s_criteria&oldid=1224304609"

WIKIPEDIA
The Free Encyclopedia

Noisy intermediate-scale quantum era

The current state of quantum computing[1] is referred to as the **noisy intermediate-scale quantum** (**NISQ**) **era**,[2][3] characterized by quantum processors containing up to 1,000 qubits which are not advanced enough yet for fault-tolerance or large enough to achieve quantum advantage.[4][5] These processors, which are sensitive to their environment (noisy) and prone to quantum decoherence, are not yet capable of continuous quantum error correction. This intermediate-scale is defined by the quantum volume, which is based on the moderate number of qubits and gate fidelity. The term NISQ was coined by John Preskill in 2018.[6][2]

According to Microsoft Azure Quantum scheme, NISQ computation is considered level 1, the lowest of the quantum computing implementation levels.[7][8]

In October 2023, the 1,000 qubit mark was passed for the first time by Atom Computing's 1,180 qubit quantum processor.[9] However, as of 2024, only two quantum processors have over 1,000 qubits, with sub-1,000 quantum processors still remaining the norm.[10]

Algorithms

NISQ algorithms are quantum algorithms designed for quantum processors in the NISQ era. Common examples are the variational quantum eigensolver (VQE) and quantum approximate optimization algorithm (QAOA), which use NISQ devices but offload some calculations to classical processors.[2] These algorithms have been successful in quantum chemistry and have potential applications in various fields including physics, materials science, data science, cryptography, biology, and finance.[2] However, due to noise during circuit execution, they often require error mitigation techniques.[11][5][12][13] These methods constitute a way of reducing the effect of noise by running a set of circuits and applying post-processing to the measured data. In contrast to quantum error correction, where errors are continuously detected and corrected during the run of the circuit, error mitigation can only use the final outcome of the noisy circuits.

Beyond-NISQ era

The creation of a computer with tens of thousands of qubits and enough error correction would eventually end the NISQ era.[4] These beyond-NISQ devices would be able to, for example, implement Shor's algorithm for very large numbers and break RSA encryption.[14]

In April 2024, researchers at Microsoft announced a significant reduction in error rates that required only 4 logical qubits, suggesting that quantum computing at scale could be years away instead of decades.[15]

See also

- Quantum complexity theory
- Quantum noise
- List of companies involved in quantum computing or communication
- List of quantum processors
- Timeline of quantum computing and communication
- Quantum information

References

1. "Quantum Computing Scientists: Give Them Lemons, They'll Make Lemonade" (http://www.aps.org/publications/apsnews/201905/quantum.cfm). *www.aps.org*. Retrieved 2021-06-29.
2. Brooks, Michael (2019-10-03). "Beyond quantum supremacy: the hunt for useful quantum computers" (https://doi.org/10.1038%2Fd41586-019-02936-3). *Nature*. **574** (7776): 19–21. Bibcode:2019Natur.574...19B (https://ui.adsabs.harvard.edu/abs/2019Natur.574...19B). doi:10.1038/d41586-019-02936-3 (https://doi.org/10.1038%2Fd41586-019-02936-3). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 31578489 (https://pubmed.ncbi.nlm.nih.gov/31578489).
3. "Quantum computers in 2023: how they work, what they do, and where they're heading" (https://theconversation.com/quantum-computers-in-2023-how-they-work-what-they-do-and-where-theyre-heading-215804). *The Conversation*. Retrieved 2024-01-15.
4. "Engineers demonstrate a quantum advantage" (https://www.sciencedaily.com/releases/2021/06/210601155610.htm). *ScienceDaily*. Retrieved 2021-06-29.
5. "What is Quantum Computing?" (https://www.techspot.com/article/2280-what-is-quantum-computing/). *TechSpot*. 28 June 2021. Retrieved 2021-06-29.
6. Preskill, John (2018-08-06). "Quantum Computing in the NISQ era and beyond" (https://quantum-journal.org/papers/q-2018-08-06-79/). *Quantum*. **2**: 79. arXiv:1801.00862 (https://arxiv.org/abs/1801.00862). Bibcode:2018Quant...2...79P (https://ui.adsabs.harvard.edu/abs/2018Quant...2...79P). doi:10.22331/q-2018-08-06-79 (https://doi.org/10.22331%2Fq-2018-08-06-79). S2CID 44098998 (https://api.semanticscholar.org/CorpusID:44098998).
7. Matt Swayne. "Microsoft Quantum's Krysta Svore Offers Glimpse Into The Quantum Future" (https://thequantuminsider.com/2023/11/01/microsoft-quantums-krysta-svore-offers-glimpse-into-the-quantum-future/). *The Quantum Insider*. Retrieved 2024-07-01.
8. "Azure Quantum | Quantum Computing Implementation Levels" (https://quantum.microsoft.com/en-us/explore/concepts/quantum-computing-implementation-levels). *quantum.microsoft.com*. Retrieved 2024-07-02.
9. Alex Wilkins. "Record-breaking quantum computer has more than 1000 qubits" (https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/). *New Scientist*. Retrieved 2024-04-18.
10. Karmela Padavic-Callaghan. "IBM's 'Condor' quantum computer has more than 1000 qubits" (https://www.newscientist.com/article/2405789-ibms-condor-quantum-computer-has-more-than-1000-qubits/). *New Scientist*. Retrieved 2024-04-18.

11. "Quantum computers are already detangling nature's mysteries" (https://www.wired.co.uk/article/quantum-computing). *Wired UK*. ISSN 1357-0978 (https://search.worldcat.org/issn/1357-0978). Retrieved 2021-06-29.
12. Ritter, Mark B. (2019). "Near-term Quantum Algorithms for Quantum Many-body Systems" (https://doi.org/10.1088%2F1742-6596%2F1290%2F1%2F012003). *Journal of Physics: Conference Series*. **1290** (1): 012003. Bibcode:2019JPhCS1290a2003R (https://ui.adsabs.harvard.edu/abs/2019JPhCS1290a2003R). doi:10.1088/1742-6596/1290/1/012003 (https://doi.org/10.1088%2F1742-6596%2F1290%2F1%2F012003). ISSN 1742-6588 (https://search.worldcat.org/issn/1742-6588).
13. Cai, Zhenyu; Babbush, Ryan; Benjamin, Simon C.; Endo, Suguru; Huggins, William J.; Li, Ying; McClean, Jarrod R.; O'Brien, Thomas E. (2023-12-13). "Quantum error mitigation" (https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.95.045005). *Rev. Mod. Phys*. **95** (3): 032338. arXiv:2210.00921 (https://arxiv.org/abs/2210.00921). doi:10.1103/RevModPhys.95.045005 (https://doi.org/10.1103%2FRevModPhys.95.045005).
14. O'Gorman, Joe; Campbell, Earl T. (2017-03-31). "Quantum computation with realistic magic-state factories" (https://link.aps.org/doi/10.1103/PhysRevA.95.032338). *Physical Review A*. **95** (3): 032338. arXiv:1605.07197 (https://arxiv.org/abs/1605.07197). Bibcode:2017PhRvA..95c2338O (https://ui.adsabs.harvard.edu/abs/2017PhRvA..95c2338O). doi:10.1103/PhysRevA.95.032338 (https://doi.org/10.1103%2FPhysRevA.95.032338). ISSN 2469-9926 (https://search.worldcat.org/issn/2469-9926). S2CID 55579588 (https://api.semanticscholar.org/CorpusID:55579588).
15. Maria Korolov. "What Microsoft's error-correction milestone means for usable quantum computing" (https://www.networkworld.com/article/2085751/what-microsofts-error-correction-milestone-means-for-usable-quantum-computing.html). *Network World*. Retrieved 2024-07-01.

External links

- John Preskill lecture on NISQ era (https://www.cornell.edu/video/john-preskill-quantum-computing-nisq-era-beyond)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Noisy_intermediate-scale_quantum_era&oldid=1232176578"

WIKIPEDIA
The Free Encyclopedia

Quantum computing

A **quantum computer** is a computer that exploits quantum mechanical phenomena. On small scales, physical matter exhibits properties of both particles and waves, and quantum computing leverages this behavior using specialized hardware. Classical physics cannot explain the operation of these quantum devices, and a scalable quantum computer could perform some calculations exponentially faster[a] than any modern "classical" computer. In particular, a large-scale quantum computer could break widely used encryption schemes and aid physicists in performing physical simulations; however, the current state of the art is largely experimental and impractical, with several obstacles to useful applications.



Quantum System One, a quantum computer by IBM from 2019 with 20 superconducting qubits[1]

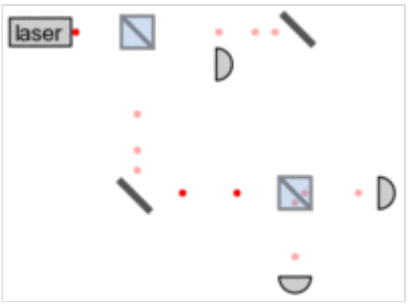
The basic unit of information in quantum computing, the qubit (or "quantum bit"), serves the same function as the bit in classical computing. However, unlike a classical bit, which can be in one of two states (a binary), a qubit can exist in a superposition of its two "basis" states, which loosely means that it is in both states simultaneously. When measuring a qubit, the result is a probabilistic output of a classical bit. If a quantum computer manipulates the qubit in a particular way, wave interference effects can amplify the desired measurement results. The design of quantum algorithms involves creating procedures that allow a quantum computer to perform calculations efficiently and quickly.

Physically engineering high-quality qubits has proven challenging. If a physical qubit is not sufficiently isolated from its environment, it suffers from quantum decoherence, introducing noise into calculations. National governments have invested heavily in experimental research that aims to develop scalable qubits with longer coherence times and lower error rates. Example implementations include superconductors (which isolate an electrical current by eliminating electrical resistance) and ion traps (which confine a single atomic particle using electromagnetic fields).

In principle, a classical computer can solve the same computational problems as a quantum computer, given enough time. Quantum advantage comes in the form of time complexity rather than computability, and quantum complexity theory shows that some quantum algorithms are exponentially more efficient than the best known classical algorithms. A large-scale quantum computer could in theory solve computational problems unsolvable by a classical computer in any reasonable amount of time. While claims of such *quantum supremacy* have drawn significant attention to the discipline, near-term practical use cases remain limited.

History

For many years, the fields of quantum mechanics and computer science formed distinct academic communities.[2] Modern quantum theory developed in the 1920s to explain the wave–particle duality observed at atomic scales,[3] and digital computers emerged in the following decades to replace human computers for tedious calculations.[4] Both disciplines had practical applications during World War II; computers played a major role in wartime cryptography,[5] and quantum physics was essential for the nuclear physics used in the Manhattan Project.[6]



The Mach–Zehnder interferometer shows that photons can exhibit wave-like interference.

As physicists applied quantum mechanical models to computational problems and swapped digital bits for qubits, the fields of quantum mechanics and computer science began to converge. In 1980, Paul Benioff introduced the quantum Turing machine, which uses quantum theory to describe a simplified computer.[7] When digital computers became faster, physicists faced an exponential increase in overhead when simulating quantum dynamics,[8] prompting Yuri Manin and Richard Feynman to independently suggest that hardware based on quantum phenomena might be more efficient for computer simulation.[9][10][11] In a 1984 paper, Charles Bennett and Gilles Brassard applied quantum theory to cryptography protocols and demonstrated that quantum key distribution could enhance information security.[12][13]

Quantum algorithms then emerged for solving oracle problems, such as Deutsch's algorithm in 1985,[14] the Bernstein–Vazirani algorithm in 1993,[15] and Simon's algorithm in 1994.[16] These algorithms did not solve practical problems, but demonstrated mathematically that one could gain more information by querying a black box with a quantum state in superposition, sometimes referred to as *quantum parallelism*.[17]

Peter Shor built on these results with his 1994 algorithm for breaking the widely used RSA and Diffie–Hellman encryption protocols,[18] which drew significant attention to the field of quantum computing.[19] In 1996, Grover's algorithm established a quantum speedup for the widely applicable unstructured search problem.[20][21] The same year, Seth Lloyd proved that quantum computers could simulate quantum systems without the exponential overhead present in classical simulations,[22] validating Feynman's 1982 conjecture.[23]


Peter Shor (pictured here in 2017) showed in 1994 that a scalable quantum computer would be able to break RSA encryption.

Over the years, experimentalists have constructed small-scale quantum computers using trapped ions and superconductors.[24] In 1998, a two-qubit quantum computer demonstrated the feasibility of the technology,[25][26] and subsequent experiments have increased the number of qubits and reduced error rates.[24]

In 2019, Google AI and NASA announced that they had achieved quantum supremacy with a 54-qubit machine, performing a computation that is impossible for any classical computer.[27][28][29] However, the validity of this claim is still being actively researched.[30][31]

The threshold theorem shows how increasing the number of qubits can mitigate errors,[32] yet fully fault-tolerant quantum computing remains "a rather distant dream".[33] According to some researchers, *noisy intermediate-scale quantum* (NISQ) machines may have specialized uses in the near future, but noise in quantum gates limits their reliability.[33]

Investment in quantum computing research has increased in the public and private sectors.[34][35] As one consulting firm summarized,[36]

> ... investment dollars are pouring in, and quantum-computing start-ups are proliferating. ... While quantum computing promises to help businesses solve problems that are beyond the reach and speed of conventional high-performance computers, use cases are largely experimental and hypothetical at this early stage.

With focus on business management's point of view, the potential applications of quantum computing into four major categories are cybersecurity, data analytics and artificial intelligence, optimization and simulation, and data management and searching.[37]

In December 2023, physicists, for the first time, reported the entanglement of individual molecules, which may have significant applications in quantum computing.[38] Also in December 2023, scientists at Harvard University successfully created "quantum circuits" that correct errors more efficiently than alternative methods, which may potentially remove a major obstacle to practical quantum computers.[39][40] The Harvard research team was supported by MIT, QuEra Computing, Caltech, and Princeton University and funded by DARPA's Optimization with Noisy Intermediate-Scale Quantum devices (ONISQ) program.[41][42] Research efforts are ongoing to jumpstart quantum computing through topological and photonic approaches as well.[43]

In July 2024, quantum computing company Quantinuum announced that their new 56-qubit H2-1 computer has broken a world record in "quantum supremacy," topping the performance of benchmarking set by Google's Sycamore machine by 100-fold and consumes 30,000 times less power.[44]

Quantum information processing

Computer engineers typically describe a modern computer's operation in terms of classical electrodynamics. Within these "classical" computers, some components (such as semiconductors and random number generators) may rely on quantum behavior, but these components are not isolated from their environment, so any quantum information quickly decoheres. While programmers may depend on probability theory when designing a randomized algorithm, quantum mechanical notions like superposition and interference are largely irrelevant for program analysis.

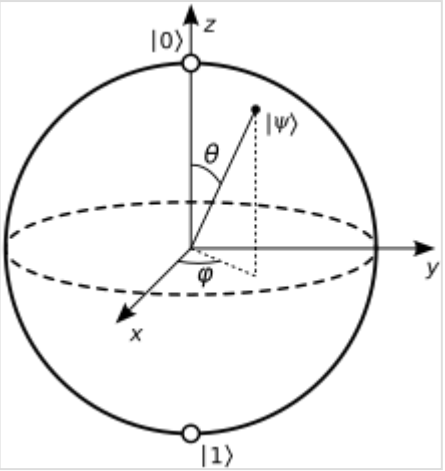
Quantum programs, in contrast, rely on precise control of coherent quantum systems. Physicists describe these systems mathematically using linear algebra. Complex numbers model probability amplitudes, vectors model quantum states, and matrices model the operations that can be performed on these states. Programming a quantum computer is then a matter of composing operations in such a way that the resulting program computes a useful result in theory and is implementable in practice.

As physicist Charlie Bennett describes the relationship between quantum and classical computers,[45]

> A classical computer is a quantum computer ... so we shouldn't be asking about "where do quantum speedups come from?" We should say, "well, all computers are quantum. ... Where do classical slowdowns come from?"

Quantum information

Just as the bit is the basic concept of classical information theory, the *qubit* is the fundamental unit of quantum information. The same term *qubit* is used to refer to an abstract mathematical model and to any physical system that is represented by that model. A classical bit, by definition, exists in either of two physical states, which can be denoted 0 and 1. A qubit is also described by a state, and two states often written $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ serve as the quantum counterparts of the classical states 0 and 1. However, the quantum states $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ belong to a vector space, meaning that they can be multiplied by constants and added together, and the result is again a valid quantum state. Such a combination is known as a *superposition* of $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$.[46][47]



Bloch sphere representation of a qubit. The state $|\psi\rangle = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$ is a point on the surface of the sphere, partway between the poles, $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$.

A two-dimensional vector mathematically represents a qubit state. Physicists typically use Dirac notation for quantum mechanical linear algebra, writing $|\psi\rangle$ 'ket psi' for a vector labeled ψ . Because a qubit is a two-state system, any qubit state takes the form $\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$, where $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ are the standard *basis states*,[b] and α and β are the *probability amplitudes*, which are in general complex numbers.[47] If either α or β is zero, the qubit is effectively a classical bit; when both are nonzero, the qubit is in superposition. Such a quantum state vector acts similarly to a (classical) probability vector, with one key difference: unlike probabilities, probability *amplitudes* are not necessarily positive numbers.[49] Negative amplitudes allow for destructive wave interference.

When a qubit is measured in the standard basis, the result is a classical bit. The Born rule describes the norm-squared correspondence between amplitudes and probabilities—when measuring a qubit $\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$, the state collapses to $|\mathbf{0}\rangle$ with probability $|\alpha|^2$, or to $|\mathbf{1}\rangle$ with probability $|\beta|^2$. Any valid qubit state has coefficients α and β such that $|\alpha|^2 + |\beta|^2 = 1$. As an example, measuring the qubit $1/\sqrt{2}|\mathbf{0}\rangle + 1/\sqrt{2}|\mathbf{1}\rangle$ would produce either $|\mathbf{0}\rangle$ or $|\mathbf{1}\rangle$ with equal probability.

Each additional qubit doubles the dimension of the state space.[48] As an example, the vector $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$ represents a two-qubit state, a tensor product of the qubit $|0\rangle$ with the qubit $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. This vector inhabits a four-dimensional vector space spanned by the basis vectors $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. The Bell state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is impossible to decompose into the tensor product of two individual qubits—the two qubits are *entangled* because their probability amplitudes are correlated. In general, the

vector space for an n-qubit system is 2^n-dimensional, and this makes it challenging for a classical computer to simulate a quantum one: representing a 100-qubit system requires storing 2^{100} classical values.

Unitary operators

The state of this one-qubit quantum memory can be manipulated by applying quantum logic gates, analogous to how classical memory can be manipulated with classical logic gates. One important gate for both classical and quantum computation is the NOT gate, which can be represented by a matrix

$$\boldsymbol{X} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Mathematically, the application of such a logic gate to a quantum state vector is modelled with matrix multiplication. Thus

$$\boldsymbol{X}|0\rangle = |1\rangle \text{ and } \boldsymbol{X}|1\rangle = |0\rangle.$$

The mathematics of single qubit gates can be extended to operate on multi-qubit quantum memories in two important ways. One way is simply to select a qubit and apply that gate to the target qubit while leaving the remainder of the memory unaffected. Another way is to apply the gate to its target only if another part of the memory is in a desired state. These two choices can be illustrated using another example. The possible states of a two-qubit quantum memory are

$$|00\rangle := \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}; \quad |01\rangle := \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}; \quad |10\rangle := \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}; \quad |11\rangle := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

The controlled NOT (CNOT) gate can then be represented using the following matrix:

$$\mathrm{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

As a mathematical consequence of this definition, $\mathrm{CNOT}\,|00\rangle = |00\rangle$, $\mathrm{CNOT}\,|01\rangle = |01\rangle$, $\mathrm{CNOT}\,|10\rangle = |11\rangle$, and $\mathrm{CNOT}\,|11\rangle = |10\rangle$. In other words, the CNOT applies a NOT gate ($\boldsymbol{X}$ from before) to the second qubit if and only if the first qubit is in the state $|1\rangle$. If the first qubit is $|0\rangle$, nothing is done to either qubit.

In summary, quantum computation can be described as a network of quantum logic gates and measurements. However, any measurement can be deferred to the end of quantum computation, though this deferment may come at a computational cost, so most quantum circuits depict a network consisting only of quantum logic gates and no measurements.

Quantum parallelism

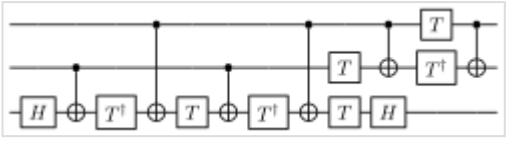
Quantum parallelism is the heuristic that quantum computers can be thought of as evaluating a function for multiple input values simultaneously. This can be achieved by preparing a quantum system in a superposition of input states, and applying a unitary transformation that encodes the function to be evaluated. The resulting state encodes the function's output values for all input values in the superposition, allowing for the computation of multiple outputs simultaneously. This property is key to the speedup of many quantum algorithms. However, "parallelism" in this sense is insufficient to speed up a computation, because the measurement at the end of the computation gives only one value. To be useful, a quantum algorithm must also incorporate some other conceptual ingredient.[50][51]

Quantum programming

There are a number of models of computation for quantum computing, distinguished by the basic elements in which the computation is decomposed.

Gate array

A quantum gate array decomposes computation into a sequence of few-qubit quantum gates. A quantum computation can be described as a network of quantum logic gates and measurements. However, any measurement can be deferred to the end of quantum computation, though this deferment may come at a computational cost, so most quantum circuits depict a network consisting only of quantum logic gates and no measurements.



A quantum circuit diagram implementing a Toffoli gate from more primitive gates

Any quantum computation (which is, in the above formalism, any unitary matrix of size $2^n \times 2^n$ over n qubits) can be represented as a network of quantum logic gates from a fairly small family of gates. A choice of gate family that enables this construction is known as a universal gate set, since a computer that can run such circuits is a universal quantum computer. One common such set includes all single-qubit gates as well as the CNOT gate from above. This means any quantum computation can be performed by executing a sequence of single-qubit gates together with CNOT gates. Though this gate set is infinite, it can be replaced with a finite gate set by appealing to the Solovay-Kitaev theorem. Implementation of Boolean functions using the few-qubit quantum gates is presented here.[52]

Measurement-based quantum computing

A measurement-based quantum computer decomposes computation into a sequence of Bell state measurements and single-qubit quantum gates applied to a highly entangled initial state (a cluster state), using a technique called quantum gate teleportation.

Adiabatic quantum computing

An adiabatic quantum computer, based on quantum annealing, decomposes computation into a slow continuous transformation of an initial Hamiltonian into a final Hamiltonian, whose ground states contain the solution.[53]

Neuromorphic quantum computing

Neuromorphic quantum computing (abbreviated as 'n.quantum computing') is an unconventional computing type of computing that uses neuromorphic computing to perform quantum operations. It was suggested that quantum algorithms, which are algorithms that run on a realistic model of quantum computation, can be computed equally efficiently with neuromorphic quantum computing. Both, traditional quantum computing and neuromorphic quantum computing are physics-based unconventional computing approaches to computations and don't follow the von Neumann architecture. They both construct a system (a circuit) that represents the physical problem at hand, and then leverage their respective physics properties of the system to seek the "minimum". Neuromorphic quantum computing and quantum computing share similar physical properties during computation.

Topological quantum computing

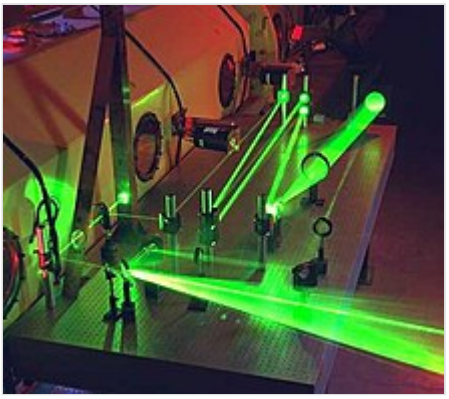
A topological quantum computer decomposes computation into the braiding of anyons in a 2D lattice.[54]

Quantum Turing machine

A quantum Turing machine is the quantum analog of a Turing machine.[7] All of these models of computation—quantum circuits,[55] one-way quantum computation,[56] adiabatic quantum computation,[57] and topological quantum computation[58]—have been shown to be equivalent to the quantum Turing machine; given a perfect implementation of one such quantum computer, it can simulate all the others with no more than polynomial overhead. This equivalence need not hold for practical quantum computers, since the overhead of simulation may be too large to be practical.

Quantum cryptography and cybersecurity

Quantum computing has significant potential applications in the fields of cryptography and cybersecurity. Quantum cryptography, which relies on the principles of quantum mechanics, offers the possibility of secure communication channels that are resistant to eavesdropping. Quantum key distribution (QKD) protocols, such as BB84, enable the secure exchange of cryptographic keys between parties, ensuring the confidentiality and integrity of communication. Moreover, quantum random number generators (QRNGs) can produce high-quality random numbers, which are essential for secure encryption.



Example of a quantum cryptosystem layout

However, quantum computing also poses challenges to traditional cryptographic systems. Shor's algorithm, a quantum algorithm for integer factorization, could potentially break widely used public-key cryptography schemes like RSA, which rely on the difficulty of factoring large numbers. Post-quantum cryptography, which involves the development of cryptographic algorithms that are resistant to attacks by both classical and quantum computers, is an active area of research aimed at addressing this concern.

Ongoing research in quantum cryptography and post-quantum cryptography is crucial for ensuring the security of communication and data in the face of evolving quantum computing capabilities. Advances in these fields, such as the development of new QKD protocols, the improvement of QRNGs, and the standardization of post-quantum cryptographic algorithms, will play a key role in maintaining the integrity and confidentiality of information in the quantum era.[59]

Communication

Quantum cryptography enables new ways to transmit data securely; for example, quantum key distribution uses entangled quantum states to establish secure cryptographic keys.[60] When a sender and receiver exchange quantum states, they can guarantee that an adversary does not intercept the message, as any unauthorized eavesdropper would disturb the delicate quantum system and introduce a detectable change.[61] With appropriate cryptographic protocols, the sender and receiver can thus establish shared private information resistant to eavesdropping.[12][62]

Modern fiber-optic cables can transmit quantum information over relatively short distances. Ongoing experimental research aims to develop more reliable hardware (such as quantum repeaters), hoping to scale this technology to long-distance quantum networks with end-to-end entanglement. Theoretically, this could enable novel technological applications, such as distributed quantum computing and enhanced quantum sensing.[63][64]

Algorithms

Progress in finding quantum algorithms typically focuses on this quantum circuit model, though exceptions like the quantum adiabatic algorithm exist. Quantum algorithms can be roughly categorized by the type of speedup achieved over corresponding classical algorithms.[65]

Quantum algorithms that offer more than a polynomial speedup over the best-known classical algorithm include Shor's algorithm for factoring and the related quantum algorithms for computing discrete logarithms, solving Pell's equation, and more generally solving the hidden subgroup problem for abelian finite groups.[65] These algorithms depend on the primitive of the quantum Fourier transform. No mathematical proof has been found that shows that an equally fast classical algorithm cannot be discovered, but evidence suggests that this is unlikely.[66] Certain oracle problems like Simon's problem and the Bernstein–Vazirani problem do give provable speedups, though this is in the quantum query model, which is a restricted model where lower bounds are much easier to prove and doesn't necessarily translate to speedups for practical problems.

Other problems, including the simulation of quantum physical processes from chemistry and solid-state physics, the approximation of certain Jones polynomials, and the quantum algorithm for linear systems of equations have quantum algorithms appearing to give super-polynomial speedups and are BQP-complete. Because these problems are BQP-complete, an equally fast classical algorithm for them would imply that *no quantum algorithm* gives a super-polynomial speedup, which is believed to be unlikely.[67]

Some quantum algorithms, like Grover's algorithm and amplitude amplification, give polynomial speedups over corresponding classical algorithms.[65] Though these algorithms give comparably modest quadratic speedup, they are widely applicable and thus give speedups for a wide range of problems.[21]

Simulation of quantum systems

Since chemistry and nanotechnology rely on understanding quantum systems, and such systems are impossible to simulate in an efficient manner classically, quantum simulation may be an important application of quantum computing.[68] Quantum simulation could also be used to simulate the behavior of atoms and particles at unusual conditions such as the reactions inside a collider.[69] In June 2023, IBM computer scientists reported that a quantum computer produced better results for a physics problem than a conventional supercomputer.[70][71]

About 2% of the annual global energy output is used for nitrogen fixation to produce ammonia for the Haber process in the agricultural fertilizer industry (even though naturally occurring organisms also produce ammonia). Quantum simulations might be used to understand this process and increase the energy efficiency of production.[72] It is expected that an early use of quantum computing will be modeling that improves the efficiency of the Haber–Bosch process[73] by the mid 2020s[74] although some have predicted it will take longer.[75]

Post-quantum cryptography

A notable application of quantum computation is for attacks on cryptographic systems that are currently in use. Integer factorization, which underpins the security of public key cryptographic systems, is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes).[76] By comparison, a quantum computer could solve this problem exponentially faster using Shor's algorithm to find its factors.[77] This ability would allow a quantum computer to break many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of digits of the integer) algorithm for solving the problem. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers or the discrete logarithm problem, both of which can be solved by Shor's algorithm. In particular, the RSA, Diffie–Hellman, and elliptic curve Diffie–Hellman algorithms could be broken. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security.

Identifying cryptographic systems that may be secure against quantum algorithms is an actively researched topic under the field of *post-quantum cryptography*.[78][79] Some public-key algorithms are based on problems other than the integer factorization and discrete logarithm problems to which Shor's algorithm applies, like the McEliece cryptosystem based on a problem in coding theory.[78][80] Lattice-based cryptosystems are also not known to be broken by quantum computers, and finding a polynomial time algorithm for solving the dihedral hidden subgroup problem, which would break many lattice based cryptosystems, is a well-studied open problem.[81] It has been proven that applying Grover's algorithm to break a symmetric (secret key) algorithm by brute force requires time equal to roughly $2^{n/2}$ invocations of

the underlying cryptographic algorithm, compared with roughly 2^n in the classical case,[82] meaning that symmetric key lengths are effectively halved: AES-256 would have the same security against an attack using Grover's algorithm that AES-128 has against classical brute-force search (see *Key size*).

Search problems

The most well-known example of a problem that allows for a polynomial quantum speedup is *unstructured search*, which involves finding a marked item out of a list of n items in a database. This can be solved by Grover's algorithm using $O(\sqrt{n})$ queries to the database, quadratically fewer than the $\Omega(n)$ queries required for classical algorithms. In this case, the advantage is not only provable but also optimal: it has been shown that Grover's algorithm gives the maximal possible probability of finding the desired element for any number of oracle lookups. Many examples of provable quantum speedups for query problems are based on Grover's algorithm, including Brassard, Høyer, and Tapp's algorithm for finding collisions in two-to-one functions,[83] and Farhi, Goldstone, and Gutmann's algorithm for evaluating NAND trees.[84]

Problems that can be efficiently addressed with Grover's algorithm have the following properties:[85][86]

1. There is no searchable structure in the collection of possible answers,
2. The number of possible answers to check is the same as the number of inputs to the algorithm, and
3. There exists a boolean function that evaluates each input and determines whether it is the correct answer.

For problems with all these properties, the running time of Grover's algorithm on a quantum computer scales as the square root of the number of inputs (or elements in the database), as opposed to the linear scaling of classical algorithms. A general class of problems to which Grover's algorithm can be applied[87] is a Boolean satisfiability problem, where the *database* through which the algorithm iterates is that of all possible answers. An example and possible application of this is a password cracker that attempts to guess a password. Breaking symmetric ciphers with this algorithm is of interest to government agencies.[88]

Quantum annealing

Quantum annealing relies on the adiabatic theorem to undertake calculations. A system is placed in the ground state for a simple Hamiltonian, which slowly evolves to a more complicated Hamiltonian whose ground state represents the solution to the problem in question. The adiabatic theorem states that if the evolution is slow enough the system will stay in its ground state at all times through the process. Adiabatic optimization may be helpful for solving computational biology problems.[89]

Machine learning

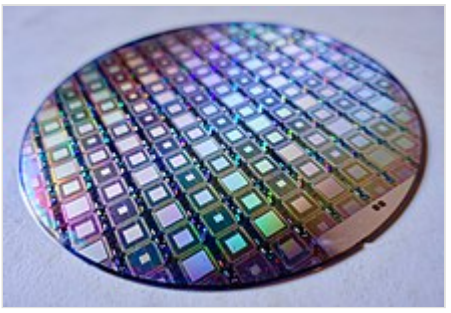
Since quantum computers can produce outputs that classical computers cannot produce efficiently, and since quantum computation is fundamentally linear algebraic, some express hope in developing quantum algorithms that can speed up machine learning tasks.[33][90]

For example, the HHL Algorithm, named after its discoverers Harrow, Hassidim, and Lloyd, is believed to provide speedup over classical counterparts.[33][91] Some research groups have recently explored the use of quantum annealing hardware for training Boltzmann machines and deep neural networks.[92][93][94]

Deep generative chemistry models emerge as powerful tools to expedite drug discovery. However, the immense size and complexity of the structural space of all possible drug-like molecules pose significant obstacles, which could be overcome in the future by quantum computers. Quantum computers are naturally good for solving complex quantum many-body problems[22] and thus may be instrumental in applications involving quantum chemistry. Therefore, one can expect that quantum-enhanced generative models[95] including quantum GANs[96] may eventually be developed into ultimate generative chemistry algorithms.

Engineering

As of 2023, classical computers outperform quantum computers for all real-world applications. While current quantum computers may speed up solutions to particular mathematical problems, they give no computational advantage for practical tasks. Scientists and engineers are exploring multiple technologies for quantum computing hardware and hope to develop scalable quantum architectures, but serious obstacles remain.[97][98]



A wafer of adiabatic quantum computers

Challenges

There are a number of technical challenges in building a large-scale quantum computer.[99] Physicist David DiVincenzo has listed these requirements for a practical quantum computer:[100]

- Physically scalable to increase the number of qubits
- Qubits that can be initialized to arbitrary values
- Quantum gates that are faster than decoherence time
- Universal gate set
- Qubits that can be read easily.

Sourcing parts for quantum computers is also very difficult. Superconducting quantum computers, like those constructed by Google and IBM, need helium-3, a nuclear research byproduct, and special superconducting cables made only by the Japanese company Coax Co.[101]

The control of multi-qubit systems requires the generation and coordination of a large number of electrical signals with tight and deterministic timing resolution. This has led to the development of quantum controllers that enable interfacing with the qubits. Scaling these systems to support a growing number of qubits is an additional challenge.[102]

Decoherence

One of the greatest challenges involved with constructing quantum computers is controlling or removing quantum decoherence. This usually means isolating the system from its environment as interactions with the external world cause the system to decohere. However, other sources of decoherence also exist. Examples include the quantum gates, and the lattice vibrations and background thermonuclear spin of the physical system used to implement the qubits. Decoherence is irreversible, as it is effectively non-unitary, and is usually something that should be highly controlled, if not avoided. Decoherence times for candidate systems in particular, the transverse relaxation time T_2 (for NMR and MRI technology, also called the *dephasing time*), typically range between nanoseconds and seconds at low temperature.[103] Currently, some quantum computers require their qubits to be cooled to 20 millikelvin (usually using a dilution refrigerator[104]) in order to prevent significant decoherence.[105] A 2020 study argues that ionizing radiation such as cosmic rays can nevertheless cause certain systems to decohere within milliseconds.[106]

As a result, time-consuming tasks may render some quantum algorithms inoperable, as attempting to maintain the state of qubits for a long enough duration will eventually corrupt the superpositions.[107]

These issues are more difficult for optical approaches as the timescales are orders of magnitude shorter and an often-cited approach to overcoming them is optical pulse shaping. Error rates are typically proportional to the ratio of operating time to decoherence time, hence any operation must be completed much more quickly than the decoherence time.

As described by the threshold theorem, if the error rate is small enough, it is thought to be possible to use quantum error correction to suppress errors and decoherence. This allows the total calculation time to be longer than the decoherence time if the error correction scheme can correct errors faster than decoherence introduces them. An often-cited figure for the required error rate in each gate for fault-tolerant computation is 10^{-3}, assuming the noise is depolarizing.

Meeting this scalability condition is possible for a wide range of systems. However, the use of error correction brings with it the cost of a greatly increased number of required qubits. The number required to factor integers using Shor's algorithm is still polynomial, and thought to be between L and L^2, where L is the number of digits in the number to be factored; error correction algorithms would inflate this figure by an additional factor of L. For a 1000-bit number, this implies a need for about 10^4 bits without error correction.[108] With error correction, the figure would rise to about 10^7 bits. Computation time is about L^2 or about 10^7 steps and at 1 MHz, about 10 seconds. However, the encoding and error-correction overheads increase the size of a real fault-tolerant quantum computer by several orders of magnitude. Careful estimates[109][110] show that at least 3 million physical qubits would factor 2,048-bit integer in 5 months on a fully error-corrected trapped-ion quantum computer. In terms of the number of physical qubits, to date, this remains the lowest estimate[111] for practically useful integer factorization problem sizing 1,024-bit or larger.

Another approach to the stability-decoherence problem is to create a topological quantum computer with anyons, quasi-particles used as threads, and relying on braid theory to form stable logic gates.[112][113]

Quantum supremacy

Physicist John Preskill coined the term *quantum supremacy* to describe the engineering feat of demonstrating that a programmable quantum device can solve a problem beyond the capabilities of state-of-the-art classical computers.[114][115][116] The problem need not be useful, so some view the quantum

supremacy test only as a potential future benchmark.[117]

In October 2019, Google AI Quantum, with the help of NASA, became the first to claim to have achieved quantum supremacy by performing calculations on the Sycamore quantum computer more than 3,000,000 times faster than they could be done on Summit, generally considered the world's fastest computer.[28][118][119] This claim has been subsequently challenged: IBM has stated that Summit can perform samples much faster than claimed,[120][121] and researchers have since developed better algorithms for the sampling problem used to claim quantum supremacy, giving substantial reductions to the gap between Sycamore and classical supercomputers[122][123][124] and even beating it.[125][126][127]

In December 2020, a group at USTC implemented a type of Boson sampling on 76 photons with a photonic quantum computer, Jiuzhang, to demonstrate quantum supremacy.[128][129][130] The authors claim that a classical contemporary supercomputer would require a computational time of 600 million years to generate the number of samples their quantum processor can generate in 20 seconds.[131]

Claims of quantum supremacy have generated hype around quantum computing,[132] but they are based on contrived benchmark tasks that do not directly imply useful real-world applications.[97][133]

In January 2024, a study published in *Physical Review Letters* provided direct verification of quantum supremacy experiments by computing exact amplitudes for experimentally generated bitstrings using a new-generation Sunway supercomputer, demonstrating a significant leap in simulation capability built on a multiple-amplitude tensor network contraction algorithm. This development underscores the evolving landscape of quantum computing, highlighting both the progress and the complexities involved in validating quantum supremacy claims.[134]

Skepticism

Despite high hopes for quantum computing, significant progress in hardware, and optimism about future applications, a 2023 Nature spotlight article summarised current quantum computers as being "For now, [good for] absolutely nothing".[97] The article elaborated that quantum computers are yet to be more useful or efficient than conventional computers in any case, though it also argued that in the long term such computers are likely to be useful. A 2023 Communications of the ACM article[98] found that current quantum computing algorithms are "insufficient for practical quantum advantage without significant improvements across the software/hardware stack". It argues that the most promising candidates for achieving speedup with quantum computers are "small-data problems", for example in chemistry and materials science. However, the article also concludes that a large range of the potential applications it considered, such as machine learning, "will not achieve quantum advantage with current quantum algorithms in the foreseeable future", and it identified I/O constraints that make speedup unlikely for "big data problems, unstructured linear systems, and database search based on Grover's algorithm".

This state of affairs can be traced to several current and long-term considerations.

- Conventional computer hardware and algorithms are not only optimized for practical tasks, but are still improving rapidly, particularly GPU accelerators.
- Current quantum computing hardware generates only a limited amount of entanglement before getting overwhelmed by noise.
- Quantum algorithms provide speedup over conventional algorithms only for some tasks, and matching these tasks with practical applications proved challenging. Some promising tasks

and applications require resources far beyond those available today.[135][136] In particular, processing large amounts of non-quantum data is a challenge for quantum computers.[98]
- Some promising algorithms have been "dequantized", i.e., their non-quantum analogues with similar complexity have been found.
- If quantum error correction is used to scale quantum computers to practical applications, its overhead may undermine speedup offered by many quantum algorithms.[98]
- Complexity analysis of algorithms sometimes makes abstract assumptions that do not hold in applications. For example, input data may not already be available encoded in quantum states, and "oracle functions" used in Grover's algorithm often have internal structure that can be exploited for faster algorithms.

In particular, building computers with large numbers of qubits may be futile if those qubits are not connected well enough and cannot maintain sufficiently high degree of entanglement for long time. When trying to outperform conventional computers, quantum computing researchers often look for new tasks that can be solved on quantum computers, but this leaves the possibility that efficient non-quantum techniques will be developed in response, as seen for Quantum supremacy demonstrations. Therefore, it is desirable to prove lower bounds on the complexity of best possible non-quantum algorithms (which may be unknown) and show that some quantum algorithms asymptomatically improve upon those bounds.

Some researchers have expressed skepticism that scalable quantum computers could ever be built, typically because of the issue of maintaining coherence at large scales, but also for other reasons.

Bill Unruh doubted the practicality of quantum computers in a paper published in 1994.[137] Paul Davies argued that a 400-qubit computer would even come into conflict with the cosmological information bound implied by the holographic principle.[138] Skeptics like Gil Kalai doubt that quantum supremacy will ever be achieved.[139][140][141] Physicist Mikhail Dyakonov has expressed skepticism of quantum computing as follows:

> "So the number of continuous parameters describing the state of such a useful quantum computer at any given moment must be... about 10^{300}... Could we ever learn to control the more than 10^{300} continuously variable parameters defining the quantum state of such a system? My answer is simple. *No, never.*"[142][143]

Physical realizations

A practical quantum computer must use a physical system as a programmable quantum register.[144] Researchers are exploring several technologies as candidates for reliable qubit implementations.[145] Superconductors and trapped ions are some of the most developed proposals, but experimentalists are considering other hardware possibilities as well.[146]

The first quantum logic gates were implemented with trapped ions and prototype general purpose machines with up to 20 qubits have been realized. However the technology behind these devices combines complex vacuum equipment, lasers, microwave and radio frequency equipment making full scale processors difficult to integrate with standard computing equipment. Moreover the trapped ion system itself has engineering challenges to overcome.[147]

The largest commercial systems are based on superconductor devices and have scaled to 2000 qubits. However the error rates for larger machines have been on the order of 5%. Technologically these devices are all cryogenic and scaling to large numbers of qubits requires wafer-scale integration, a serious engineering challenge by itself.[148]

Theory

Computability

Any computational problem solvable by a classical computer is also solvable by a quantum computer.[149] Intuitively, this is because it is believed that all physical phenomena, including the operation of classical computers, can be described using quantum mechanics, which underlies the operation of quantum computers.

Conversely, any problem solvable by a quantum computer is also solvable by a classical computer. It is possible to simulate both quantum and classical computers manually with just some paper and a pen, if given enough time. More formally, any quantum computer can be simulated by a Turing machine. In other words, quantum computers provide no additional power over classical computers in terms of computability. This means that quantum computers cannot solve undecidable problems like the halting problem, and the existence of quantum computers does not disprove the Church–Turing thesis.[150]

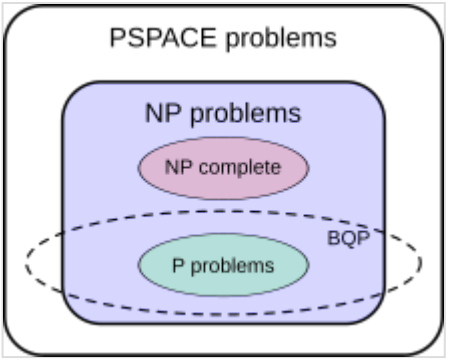
Complexity

While quantum computers cannot solve any problems that classical computers cannot already solve, it is suspected that they can solve certain problems faster than classical computers. For instance, it is known that quantum computers can efficiently factor integers, while this is not believed to be the case for classical computers.

The class of problems that can be efficiently solved by a quantum computer with bounded error is called BQP, for "bounded error, quantum, polynomial time". More formally, BQP is the class of problems that can be solved by a polynomial-time quantum Turing machine with an error probability of at most 1/3. As a class of probabilistic problems, BQP is the quantum counterpart to BPP ("bounded error, probabilistic, polynomial time"), the class of problems that can be solved by polynomial-time probabilistic Turing machines with bounded error.[151] It is known that $\mathsf{BPP} \subseteq \mathsf{BQP}$ and is widely suspected that $\mathsf{BQP} \subsetneq \mathsf{BPP}$, which intuitively would mean that quantum computers are more powerful than classical computers in terms of time complexity.[152]

The exact relationship of BQP to P, NP, and PSPACE is not known. However, it is known that $\mathsf{P} \subseteq \mathsf{BQP} \subseteq \mathsf{PSPACE}$; that is, all problems that can be efficiently solved by a deterministic classical computer can also be efficiently solved by a quantum computer, and all problems that can be efficiently solved by a quantum computer can also be solved by a deterministic classical computer with polynomial space resources. It is further suspected that BQP is a strict superset of P, meaning there are problems that are efficiently solvable by quantum computers that are not efficiently solvable by deterministic classical computers. For instance, integer factorization and the discrete logarithm problem are known to be in BQP and are suspected to be outside of P. On the relationship of BQP to NP, little is known beyond the fact that some NP problems that are believed not to be in P are also in BQP (integer factorization and the discrete

logarithm problem are both in NP, for example). It is suspected that $\mathbf{NP} \not\subseteq \mathbf{BQP}$; that is, it is believed that there are efficiently checkable problems that are not efficiently solvable by a quantum computer. As a direct consequence of this belief, it is also suspected that BQP is disjoint from the class of NP-complete problems (if an NP-complete problem were in BQP, then it would follow from NP-hardness that all problems in NP are in BQP).[153]



The suspected relationship of BQP to several classical complexity classes[67]

See also

- D-Wave Systems – Canadian quantum computing company
- Electronic quantum holography
- Glossary of quantum computing
- IARPA – American government agency
- IonQ – US information technology company
- List of emerging technologies – New technologies actively in development
- List of quantum processors – List of quantum computer components
- Magic state distillation – Quantum computing algorithm
- Natural computing – terminology introduced to encompass three classes of methods
- Optical computing – Computer that uses photons or light waves
- Quantum bus – device which can be used to store or transfer information between independent qubits in a quantum computer
- Quantum cognition – Application of quantum theory mathematics to cognitive phenomena
- Quantum volume – Metric for a quantum computer's capabilities
- Quantum weirdness – Unintuitive aspects of quantum mechanics
- Rigetti Computing – American quantum computing company
- Supercomputer – Type of extremely powerful computer
- Theoretical computer science – Subfield of computer science and mathematics
- Unconventional computing – Computing by new or unusual methods
- Valleytronics – Experimental area in semiconductors

Notes

a. As used in this article, "exponentially faster" has a precise complexity theoretical meaning. Usually, it means that as a function of input size in bits, the best known classical algorithm

for a problem requires an exponentially growing number of steps, while a quantum algorithm uses only a polynomial number of steps.

b. The standard basis is also the *computational basis*.[48]

References

1. Russell, John (10 January 2019). "IBM Quantum Update: Q System One Launch, New Collaborators, and QC Center Plans" (https://www.hpcwire.com/2019/01/10/ibm-quantum-update-q-system-one-launch-new-collaborators-and-qc-center-plans/). *HPCwire*. Retrieved 9 January 2023.
2. Aaronson 2013, p. 132.
3. Bhatta, Varun S. (10 May 2020). "Plurality of Wave–Particle Duality" (https://www.currentscience.ac.in/Volumes/118/09/1365.pdf) (PDF). *Current Science*. **118** (9): 1365. doi:10.18520/cs/v118/i9/1365-1374 (https://doi.org/10.18520%2Fcs%2Fv118%2Fi9%2F1365-1374). ISSN 0011-3891 (https://search.worldcat.org/issn/0011-3891). S2CID 216143449 (https://api.semanticscholar.org/CorpusID:216143449).
4. Ceruzzi, Paul E. (2012). *Computing: A Concise History*. Cambridge, Massachusetts: MIT Press. pp. 3, 46. ISBN 978-0-262-31038-3. OCLC 796812982 (https://search.worldcat.org/oclc/796812982).
5. Hodges, Andrew (2014). *Alan Turing: The Enigma*. Princeton, New Jersey: Princeton University Press. p. xviii. ISBN 9780691164724.
6. Mårtensson-Pendrill, Ann-Marie (1 November 2006). "The Manhattan project—a part of physics history". *Physics Education*. **41** (6): 493–501. Bibcode:2006PhyEd..41..493M (https://ui.adsabs.harvard.edu/abs/2006PhyEd..41..493M). doi:10.1088/0031-9120/41/6/001 (https://doi.org/10.1088%2F0031-9120%2F41%2F6%2F001). ISSN 0031-9120 (https://search.worldcat.org/issn/0031-9120). S2CID 120294023 (https://api.semanticscholar.org/CorpusID:120294023).
7. Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". *Journal of Statistical Physics*. **22** (5): 563–591. Bibcode:1980JSP....22..563B (https://ui.adsabs.harvard.edu/abs/1980JSP....22..563B). doi:10.1007/bf01011339 (https://doi.org/10.1007%2Fbf01011339). S2CID 122949592 (https://api.semanticscholar.org/CorpusID:122949592).
8. Buluta, Iulia; Nori, Franco (2 October 2009). "Quantum Simulators". *Science*. **326** (5949): 108–111. Bibcode:2009Sci...326..108B (https://ui.adsabs.harvard.edu/abs/2009Sci...326..108B). doi:10.1126/science.1177838 (https://doi.org/10.1126%2Fscience.1177838). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 19797653 (https://pubmed.ncbi.nlm.nih.gov/19797653). S2CID 17187000 (https://api.semanticscholar.org/CorpusID:17187000).
9. Manin, Yu. I. (1980). *Vychislimoe i nevychislimoe* (https://web.archive.org/web/20130510173823/http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) [*Computable and Noncomputable*] (in Russian). Soviet Radio. pp. 13–15. Archived from the original (http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5bdjv-fax%5d.zip) on 10 May 2013. Retrieved 4 March 2013.

10. Feynman, Richard (June 1982). "Simulating Physics with Computers" (https://web.archive.org/web/20190108115138/https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf) (PDF). *International Journal of Theoretical Physics*. **21** (6/7): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445). Archived from the original (https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf) (PDF) on 8 January 2019. Retrieved 28 February 2019.
11. Nielsen & Chuang 2010, p. 214.
12. Bennett, Charles H.; Brassard, Gilles (December 1984). *Quantum cryptography: Public key distribution and coin tossing*. IEEE International Conference on Computers, Systems & Signal Processing. Bangalore, India. pp. 175–179. arXiv:2003.06557 (https://arxiv.org/abs/2003.06557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025).
13. Brassard, G. (2005). "Brief history of quantum cryptography: A personal perspective" (https://ieeexplore.ieee.org/document/1543949). *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005*. Awaji Island, Japan: IEEE. pp. 19–23. arXiv:quant-ph/0604072 (https://arxiv.org/abs/quant-ph/0604072). doi:10.1109/ITWTPI.2005.1543949 (https://doi.org/10.1109%2FITWTPI.2005.1543949). ISBN 978-0-7803-9491-9. S2CID 16118245 (https://api.semanticscholar.org/CorpusID:16118245).
14. Deutsch, D. (8 July 1985). "Quantum theory, the Church–Turing principle and the universal quantum computer". *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D (https://ui.adsabs.harvard.edu/abs/1985RSPSA.400...97D). doi:10.1098/rspa.1985.0070 (https://doi.org/10.1098%2Frspa.1985.0070). ISSN 0080-4630 (https://search.worldcat.org/issn/0080-4630). S2CID 1438116 (https://api.semanticscholar.org/CorpusID:1438116).
15. Bernstein, Ethan; Vazirani, Umesh (1993). "Quantum complexity theory" (http://portal.acm.org/citation.cfm?doid=167088.167097). *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing – STOC '93*. San Diego, California, United States: ACM Press. pp. 11–20. doi:10.1145/167088.167097 (https://doi.org/10.1145%2F167088.167097). ISBN 978-0-89791-591-5. S2CID 676378 (https://api.semanticscholar.org/CorpusID:676378).
16. Simon, D. R. (1994). "On the power of quantum computation" (https://ieeexplore.ieee.org/document/365701). *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, New Mexico, USA: IEEE Comput. Soc. Press. pp. 116–123. doi:10.1109/SFCS.1994.365701 (https://doi.org/10.1109%2FSFCS.1994.365701). ISBN 978-0-8186-6580-6. S2CID 7457814 (https://api.semanticscholar.org/CorpusID:7457814).
17. Nielsen & Chuang 2010, p. 30-32.
18. Shor 1994.
19. Grumbling & Horowitz 2019, p. 15.
20. Grover, Lov K. (1996). *A fast quantum mechanical algorithm for database search*. ACM symposium on Theory of computing. Philadelphia: ACM Press. pp. 212–219. arXiv:quant-ph/9605043 (https://arxiv.org/abs/quant-ph/9605043). doi:10.1145/237814.237866 (https://doi.org/10.1145%2F237814.237866). ISBN 978-0-89791-785-8.
21. Nielsen & Chuang 2010, p. 7.
22. Lloyd, Seth (23 August 1996). "Universal Quantum Simulators". *Science*. **273** (5278): 1073–1078. Bibcode:1996Sci...273.1073L (https://ui.adsabs.harvard.edu/abs/1996Sci...273.1073L). doi:10.1126/science.273.5278.1073 (https://doi.org/10.1126%2Fscience.273.5278.1073). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 8688088 (https://pubmed.ncbi.nlm.nih.gov/8688088). S2CID 43496899 (https://api.semanticscholar.org/CorpusID:43496899).

23. Cao, Yudong; Romero, Jonathan; Olson, Jonathan P.; Degroote, Matthias; Johnson, Peter D.; et al. (9 October 2019). "Quantum Chemistry in the Age of Quantum Computing". *Chemical Reviews*. **119** (19): 10856–10915. arXiv:1812.09976 (https://arxiv.org/abs/1812.09976). doi:10.1021/acs.chemrev.8b00803 (https://doi.org/10.1021%2Facs.chemrev.8b00803). ISSN 0009-2665 (https://search.worldcat.org/issn/0009-2665). PMID 31469277 (https://pubmed.ncbi.nlm.nih.gov/31469277). S2CID 119417908 (https://api.semanticscholar.org/CorpusID:119417908).
24. Grumbling & Horowitz 2019, pp. 164–169.
25. Chuang, Isaac L.; Gershenfeld, Neil; Kubinec, Markdoi (April 1998). "Experimental Implementation of Fast Quantum Searching". *Physical Review Letters*. **80** (15). American Physical Society: 3408–3411. Bibcode:1998PhRvL..80.3408C (https://ui.adsabs.harvard.edu/abs/1998PhRvL..80.3408C). doi:10.1103/PhysRevLett.80.3408 (https://doi.org/10.1103%2FPhysRevLett.80.3408).
26. Holton, William Coffeen. "quantum computer" (https://www.britannica.com/technology/quantum-computer). *Encyclopedia Britannica*. Encyclopædia Britannica. Retrieved 4 December 2021.
27. Gibney, Elizabeth (23 October 2019). "Hello quantum world! Google publishes landmark quantum supremacy claim" (https://doi.org/10.1038%2Fd41586-019-03213-z). *Nature*. **574** (7779): 461–462. Bibcode:2019Natur.574..461G (https://ui.adsabs.harvard.edu/abs/2019Natur.574..461G). doi:10.1038/d41586-019-03213-z (https://doi.org/10.1038%2Fd41586-019-03213-z). PMID 31645740 (https://pubmed.ncbi.nlm.nih.gov/31645740).
28. Lay summary: Martinis, John; Boixo, Sergio (23 October 2019). "Quantum Supremacy Using a Programmable Superconducting Processor" (https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html). *Nature*. **574** (7779). Google AI: 505–510. arXiv:1910.11333 (https://arxiv.org/abs/1910.11333). Bibcode:2019Natur.574..505A (https://ui.adsabs.harvard.edu/abs/2019Natur.574..505A). doi:10.1038/s41586-019-1666-5 (https://doi.org/10.1038%2Fs41586-019-1666-5). PMID 31645734 (https://pubmed.ncbi.nlm.nih.gov/31645734). S2CID 204836822 (https://api.semanticscholar.org/CorpusID:204836822). Retrieved 27 April 2022.
    • Journal article: Arute, Frank; Arya, Kunal; Babbush, Ryan; Bacon, Dave; Bardin, Joseph C.; et al. (23 October 2019). "Quantum supremacy using a programmable superconducting processor". *Nature*. **574** (7779): 505–510. arXiv:1910.11333 (https://arxiv.org/abs/1910.11333). Bibcode:2019Natur.574..505A (https://ui.adsabs.harvard.edu/abs/2019Natur.574..505A). doi:10.1038/s41586-019-1666-5 (https://doi.org/10.1038%2Fs41586-019-1666-5). PMID 31645734 (https://pubmed.ncbi.nlm.nih.gov/31645734). S2CID 204836822 (https://api.semanticscholar.org/CorpusID:204836822).
29. Aaronson, Scott (30 October 2019). "Opinion | Why Google's Quantum Supremacy Milestone Matters" (https://www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html). *The New York Times*. ISSN 0362-4331 (https://search.worldcat.org/issn/0362-4331). Retrieved 25 September 2021.
30. Pednault, Edwin (22 October 2019). "On 'Quantum Supremacy' " (https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/). *IBM Research Blog*. Retrieved 9 February 2021.
31. Pan, Feng; Zhang, Pan (4 March 2021). "Simulating the Sycamore quantum supremacy circuits". arXiv:2103.03074 (https://arxiv.org/abs/2103.03074) [quant-ph (https://arxiv.org/archive/quant-ph)].
32. Nielsen & Chuang 2010, p. 481.
33. Preskill, John (6 August 2018). "Quantum Computing in the NISQ era and beyond" (https://doi.org/10.22331%2Fq-2018-08-06-79). *Quantum*. **2**: 79. arXiv:1801.00862 (https://arxiv.org/abs/1801.00862). Bibcode:2018Quant...2...79P (https://ui.adsabs.harvard.edu/abs/2018Quant...2...79P). doi:10.22331/q-2018-08-06-79 (https://doi.org/10.22331%2Fq-2018-08-06-79). S2CID 44098998 (https://api.semanticscholar.org/CorpusID:44098998).

34. Gibney, Elizabeth (2 October 2019). "Quantum gold rush: the private funding pouring into quantum start-ups". *Nature*. **574** (7776): 22–24. Bibcode:2019Natur.574...22G (https://ui.adsabs.harvard.edu/abs/2019Natur.574...22G). doi:10.1038/d41586-019-02935-4 (https://doi.org/10.1038%2Fd41586-019-02935-4). PMID 31578480 (https://pubmed.ncbi.nlm.nih.gov/31578480). S2CID 203626236 (https://api.semanticscholar.org/CorpusID:203626236).
35. Rodrigo, Chris Mills (12 February 2020). "Trump budget proposal boosts funding for artificial intelligence, quantum computing" (https://thehill.com/policy/technology/482402-trump-budget-proposal-boosts-funding-for-artificial-intelligence-quantum). *The Hill*. Retrieved 11 July 2021.
36. Biondi, Matteo; Heid, Anna; Henke, Nicolaus; Mohr, Niko; Pautasso, Lorenzo; et al. (14 December 2021). "Quantum computing use cases are getting real—what you need to know" (https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know). *McKinsey & Company*. Retrieved 1 April 2022.
37. Leong, Kelvin; Sung, Anna (November 2022). "What Business Managers Should Know About Quantum Computing?" (http://journalofinterdisciplinarysciences.com/wp-content/uploads/2022/10/3-What-Business-Managers-Should-Know-About-Quantum-Computing.pdf) (PDF). *Journal of Interdisciplinary Sciences*. Retrieved 13 August 2023.
38. Staff (7 December 2023). "Physicists 'entangle' individual molecules for the first time, hastening possibilities for quantum computing" (https://phys.org/news/2023-12-physicists-entangle-individual-molecules-hastening.html). *Phys.org*. Archived (https://archive.today/20231208152543/https://phys.org/news/2023-12-physicists-entangle-individual-molecules-hastening.html) from the original on 8 December 2023. Retrieved 8 December 2023.
39. Bluvstein, Dolev; Evered, Simon J.; Geim, Alexandra A.; Li, Sophie H.; Zhou, Hengyun; Manovitz, Tom; Ebadi, Sepehr; Cain, Madelyn; Kalinowski, Marcin; Hangleiter, Dominik; Ataides, J. Pablo Bonilla; Maskara, Nishad; Cong, Iris; Gao, Xun; Rodriguez, Pedro Sales (6 December 2023). "Logical quantum processor based on reconfigurable atom arrays" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). *Nature*. **626** (7997): 58–65. arXiv:2312.03982 (https://arxiv.org/abs/2312.03982). doi:10.1038/s41586-023-06927-3 (https://doi.org/10.1038%2Fs41586-023-06927-3). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 10830422 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). PMID 38056497 (https://pubmed.ncbi.nlm.nih.gov/38056497). S2CID 266052773 (https://api.semanticscholar.org/CorpusID:266052773).
40. Freedberg Jr., Sydney J. (7 December 2023). " 'Off to the races': DARPA, Harvard breakthrough brings quantum computing years closer" (https://breakingdefense.sites.breakingmedia.com/2023/12/off-to-the-races-darpa-harvard-breakthrough-brings-quantum-computing-years-closer/). *Breaking Defense*. Retrieved 9 December 2023.
41. "DARPA-Funded Research Leads to Quantum Computing Breakthrough" (https://www.darpa.mil/news-events/2023-12-06). *darpa.mil*. 6 December 2023. Retrieved 5 January 2024.
42. Choudhury, Rizwan (30 December 2023). "Top 7 innovation stories of 2023 – Interesting Engineering" (https://interestingengineering.com/lists/top-7-innovation-stories-of-2023-interesting-engineering). *interestingengineering.com*. Retrieved 6 January 2024.
43. Mackie, Kurt (8 February 2024). "Microsoft Quantum Computing Getting DARPA Funding" (https://rcpmag.com/Articles/2024/02/08/Microsoft-Quantum-Computing-DARPA.aspx). *rcpmag.com*. Retrieved 9 February 2024.
44. Keumars Afifi-Sabet (11 July 2024). "New quantum computer smashes 'quantum supremacy' record by a factor of 100 — and it consumes 30,000 times less power" (https://www.livescience.com/technology/computing/new-quantum-computer-smashes-quantum-supremacy-record-by-a-factor-of-100-and-it-consumes-30000-times-less-power). *livescience.com*. Retrieved 11 July 2024.
45. Bennett, Charlie (31 July 2020). *Information Is Quantum: How Physics Helped Explain the Nature of Information and What Can Be Done With It* (https://www.youtube.com/live/rslt-LwtDK4&t=4102) (Videotape). Event occurs at 1:08:22 – via YouTube.

46. Nielsen & Chuang 2010, p. 13.
47. Mermin 2007, p. 17.
48. Mermin 2007, p. 18.
49. Aaronson 2013, p. 110.
50. Nielsen & Chuang 2010, p. 30–32.
51. Mermin 2007, pp. 38–39.
52. Kurgalin, Sergei; Borzunov, Sergei (2021). *Concise guide to quantum computing: algorithms, exercises, and implementations*. Texts in computer science. Cham: Springer. ISBN 978-3-030-65054-4.
53. Das, A.; Chakrabarti, B. K. (2008). "Quantum Annealing and Analog Quantum Computation". *Rev. Mod. Phys.* **80** (3): 1061–1081. arXiv:0801.2193 (https://arxiv.org/abs/0801.2193). Bibcode:2008RvMP...80.1061D (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1061D). CiteSeerX 10.1.1.563.9990 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.563.9990). doi:10.1103/RevModPhys.80.1061 (https://doi.org/10.1103%2FRevModPhys.80.1061). S2CID 14255125 (https://api.semanticscholar.org/CorpusID:14255125).
54. Nayak, Chetan; Simon, Steven; Stern, Ady; Das Sarma, Sankar (2008). "Nonabelian Anyons and Quantum Computation". *Reviews of Modern Physics*. **80** (3): 1083–1159. arXiv:0707.1889 (https://arxiv.org/abs/0707.1889). Bibcode:2008RvMP...80.1083N (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1083N). doi:10.1103/RevModPhys.80.1083 (https://doi.org/10.1103%2FRevModPhys.80.1083). S2CID 119628297 (https://api.semanticscholar.org/CorpusID:119628297).
55. Chi-Chih Yao, A. (1993). "Quantum circuit complexity" (https://ieeexplore.ieee.org/document/366852). *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*. pp. 352–361. doi:10.1109/SFCS.1993.366852 (https://doi.org/10.1109%2FSFCS.1993.366852). ISBN 0-8186-4370-6. S2CID 195866146 (https://api.semanticscholar.org/CorpusID:195866146).
56. Raussendorf, Robert; Browne, Daniel E.; Briegel, Hans J. (25 August 2003). "Measurement-based quantum computation on cluster states". *Physical Review A*. **68** (2): 022312. arXiv:quant-ph/0301052 (https://arxiv.org/abs/quant-ph/0301052). Bibcode:2003PhRvA..68b2312R (https://ui.adsabs.harvard.edu/abs/2003PhRvA..68b2312R). doi:10.1103/PhysRevA.68.022312 (https://doi.org/10.1103%2FPhysRevA.68.022312). S2CID 6197709 (https://api.semanticscholar.org/CorpusID:6197709).
57. Aharonov, Dorit; van Dam, Wim; Kempe, Julia; Landau, Zeph; Lloyd, Seth; Regev, Oded (1 January 2008). "Adiabatic Quantum Computation Is Equivalent to Standard Quantum Computation". *SIAM Review*. **50** (4): 755–787. arXiv:quant-ph/0405098 (https://arxiv.org/abs/quant-ph/0405098). Bibcode:2008SIAMR..50..755A (https://ui.adsabs.harvard.edu/abs/2008SIAMR..50..755A). doi:10.1137/080734479 (https://doi.org/10.1137%2F080734479). ISSN 0036-1445 (https://search.worldcat.org/issn/0036-1445). S2CID 1503123 (https://api.semanticscholar.org/CorpusID:1503123).
58. Freedman, Michael H.; Larsen, Michael; Wang, Zhenghan (1 June 2002). "A Modular Functor Which is Universal for Quantum Computation". *Communications in Mathematical Physics*. **227** (3): 605–622. arXiv:quant-ph/0001108 (https://arxiv.org/abs/quant-ph/0001108). Bibcode:2002CMaPh.227..605F (https://ui.adsabs.harvard.edu/abs/2002CMaPh.227..605F). doi:10.1007/s002200200645 (https://doi.org/10.1007%2Fs002200200645). ISSN 0010-3616 (https://search.worldcat.org/issn/0010-3616). S2CID 8990600 (https://api.semanticscholar.org/CorpusID:8990600).

59. Pirandola, S.; Andersen, U. L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; Pereira, J.; Razavi, M.; Shamsul Shaari, J.; Tomamichel, M.; Usenko, V. C.; Vallone, G.; Villoresi, P.; Wallden, P. (2020). "Advances in quantum cryptography". *Advances in Optics and Photonics*. **12** (4): 1012–1236. arXiv:1906.01645 (https://arxiv.org/abs/1906.01645). Bibcode:2020AdOP...12.1012P (https://ui.adsabs.harvard.edu/abs/2020AdOP...12.1012P). doi:10.1364/AOP.361502 (https://doi.org/10.1364%2FAOP.361502).
60. Pirandola, S.; Andersen, U. L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; Pereira, J. L.; Razavi, M.; Shamsul Shaari, J.; Tomamichel, M.; Usenko, V. C. (14 December 2020). "Advances in quantum cryptography". *Advances in Optics and Photonics*. **12** (4): 1017. arXiv:1906.01645 (https://arxiv.org/abs/1906.01645). Bibcode:2020AdOP...12.1012P (https://ui.adsabs.harvard.edu/abs/2020AdOP...12.1012P). doi:10.1364/AOP.361502 (https://doi.org/10.1364%2FAOP.361502). ISSN 1943-8206 (https://search.worldcat.org/issn/1943-8206). S2CID 174799187 (https://api.semanticscholar.org/CorpusID:174799187).
61. Xu, Feihu; Ma, Xiongfeng; Zhang, Qiang; Lo, Hoi-Kwong; Pan, Jian-Wei (26 May 2020). "Secure quantum key distribution with realistic devices". *Reviews of Modern Physics*. **92** (2): 025002-3. arXiv:1903.09051 (https://arxiv.org/abs/1903.09051). Bibcode:2020RvMP...92b5002X (https://ui.adsabs.harvard.edu/abs/2020RvMP...92b5002X). doi:10.1103/RevModPhys.92.025002 (https://doi.org/10.1103%2FRevModPhys.92.025002). S2CID 210942877 (https://api.semanticscholar.org/CorpusID:210942877).
62. Xu, Guobin; Mao, Jianzhou; Sakk, Eric; Wang, Shuangbao Paul (22 March 2023). "An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography". *2023 57th Annual Conference on Information Sciences and Systems (CISS)*. IEEE. p. 3. doi:10.1109/CISS56502.2023.10089619 (https://doi.org/10.1109%2FCISS56502.2023.10089619). ISBN 978-1-6654-5181-9.
63. Kozlowski, Wojciech; Wehner, Stephanie (25 September 2019). "Towards Large-Scale Quantum Networks". *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication*. ACM. pp. 1–7. arXiv:1909.08396 (https://arxiv.org/abs/1909.08396). doi:10.1145/3345312.3345497 (https://doi.org/10.1145%2F3345312.3345497). ISBN 978-1-4503-6897-1.
64. Guo, Xueshi; Breum, Casper R.; Borregaard, Johannes; Izumi, Shuro; Larsen, Mikkel V.; Gehring, Tobias; Christandl, Matthias; Neergaard-Nielsen, Jonas S.; Andersen, Ulrik L. (23 December 2019). "Distributed quantum sensing in a continuous-variable entangled network". *Nature Physics*. **16** (3): 281–284. arXiv:1905.09408 (https://arxiv.org/abs/1905.09408). doi:10.1038/s41567-019-0743-x (https://doi.org/10.1038%2Fs41567-019-0743-x). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 256703226 (https://api.semanticscholar.org/CorpusID:256703226).
65. Jordan, Stephen (14 October 2022) [22 April 2011]. "Quantum Algorithm Zoo" (http://math.nist.gov/quantum/zoo/). Archived (https://web.archive.org/web/20180429014516/https://math.nist.gov/quantum/zoo/) from the original on 29 April 2018.
66. Aaronson, Scott; Arkhipov, Alex (6 June 2011). "The computational complexity of linear optics". *Proceedings of the forty-third annual ACM symposium on Theory of computing*. San Jose, California: Association for Computing Machinery. pp. 333–342. arXiv:1011.3245 (https://arxiv.org/abs/1011.3245). doi:10.1145/1993636.1993682 (https://doi.org/10.1145%2F1993636.1993682). ISBN 978-1-4503-0691-1.
67. Nielsen & Chuang 2010, p. 42.
68. Norton, Quinn (15 February 2007). "The Father of Quantum Computing" (http://archive.wired.com/science/discoveries/news/2007/02/72734). *Wired*.
69. Ambainis, Andris (Spring 2014). "What Can We Do with a Quantum Computer?" (http://www.ias.edu/ias-letter/ambainis-quantum-computing). Institute for Advanced Study.

70. Chang, Kenneth (14 June 2023). "Quantum Computing Advance Begins New Era, IBM Says – A quantum computer came up with better answers to a physics problem than a conventional supercomputer" (https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html). *The New York Times*. Archived (https://archive.today/20230614151835/https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html) from the original on 14 June 2023. Retrieved 15 June 2023.
71. Kim, Youngseok; et al. (14 June 2023). "Evidence for the utility of quantum computing before fault tolerance" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10266970). *Nature*. **618** (7965): 500–505. Bibcode:2023Natur.618..500K (https://ui.adsabs.harvard.edu/abs/2023Natur.618..500K). doi:10.1038/s41586-023-06096-3 (https://doi.org/10.1038%2Fs41586-023-06096-3). PMC 10266970 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10266970). PMID 37316724 (https://pubmed.ncbi.nlm.nih.gov/37316724).
72. Morello, Andrea (21 November 2018). *Lunch & Learn: Quantum Computing* (https://web.archive.org/web/20210215140237/https://www.youtube.com/watch?v=7susESgnDv8). Sibos TV. Archived from the original on 15 February 2021. Retrieved 4 February 2021 – via YouTube.
73. Ruane, Jonathan; McAfee, Andrew; Oliver, William D. (1 January 2022). "Quantum Computing for Business Leaders" (https://hbr.org/2022/01/quantum-computing-for-business-leaders). *Harvard Business Review*. ISSN 0017-8012 (https://search.worldcat.org/issn/0017-8012). Retrieved 12 April 2023.
74. Budde, Florian; Volz, Daniel (12 July 2019). "Quantum computing and the chemical industry | McKinsey" (https://www.mckinsey.com/industries/chemicals/our-insights/the-next-big-thing-quantum-computings-potential-impact-on-chemicals). *www.mckinsey.com*. McKinsey and Company. Retrieved 12 April 2023.
75. Bourzac, Katherine (30 October 2017). "Chemistry is quantum computing's killer app" (https://cen.acs.org/articles/95/i43/Chemistry-quantum-computings-killer-app.html). *cen.acs.org*. American Chemical Society. Retrieved 12 April 2023.
76. Lenstra, Arjen K. (2000). "Integer Factoring" (https://web.archive.org/web/20150410234239/http://sage.math.washington.edu/edu/124/misc/arjen_lenstra_factoring.pdf) (PDF). *Designs, Codes and Cryptography*. **19** (2/3): 101–128. doi:10.1023/A:1008397921377 (https://doi.org/10.1023%2FA%3A1008397921377). S2CID 9816153 (https://api.semanticscholar.org/CorpusID:9816153). Archived from the original (http://sage.math.washington.edu/edu/124/misc/arjen_lenstra_factoring.pdf) (PDF) on 10 April 2015.
77. Nielsen & Chuang 2010, p. 216.
78. Bernstein, Daniel J. (2009). "Introduction to post-quantum cryptography". *Post-Quantum Cryptography*. Berlin, Heidelberg: Springer. pp. 1–14. doi:10.1007/978-3-540-88702-7_1 (https://doi.org/10.1007%2F978-3-540-88702-7_1). ISBN 978-3-540-88701-0. S2CID 61401925 (https://api.semanticscholar.org/CorpusID:61401925).
79. See also pqcrypto.org (http://pqcrypto.org/), a bibliography maintained by Daniel J. Bernstein and Tanja Lange on cryptography not known to be broken by quantum computing.
80. McEliece, R. J. (January 1978). "A Public-Key Cryptosystem Based On Algebraic Coding Theory" (http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF) (PDF). *DSNPR*. **44**: 114–116. Bibcode:1978DSNPR..44..114M (https://ui.adsabs.harvard.edu/abs/1978DSNPR..44..114M).
81. Kobayashi, H.; Gall, F. L. (2006). "Dihedral Hidden Subgroup Problem: A Survey" (https://doi.org/10.2197%2Fipsjdc.1.470). *Information and Media Technologies*. **1** (1): 178–185. doi:10.2197/ipsjdc.1.470 (https://doi.org/10.2197%2Fipsjdc.1.470).

82. Bennett, Charles H.; Bernstein, Ethan; Brassard, Gilles; Vazirani, Umesh (October 1997). "Strengths and Weaknesses of Quantum Computing". *SIAM Journal on Computing*. **26** (5): 1510–1523. arXiv:quant-ph/9701001 (https://arxiv.org/abs/quant-ph/9701001). Bibcode:1997quant.ph..1001B (https://ui.adsabs.harvard.edu/abs/1997quant.ph..1001B). doi:10.1137/s0097539796300933 (https://doi.org/10.1137%2Fs0097539796300933). S2CID 13403194 (https://api.semanticscholar.org/CorpusID:13403194).
83. Brassard, Gilles; Høyer, Peter; Tapp, Alain (2016). "Quantum Algorithm for the Collision Problem". In Kao, Ming-Yang (ed.). *Encyclopedia of Algorithms*. New York, New York: Springer. pp. 1662–1664. arXiv:quant-ph/9705002 (https://arxiv.org/abs/quant-ph/9705002). doi:10.1007/978-1-4939-2864-4_304 (https://doi.org/10.1007%2F978-1-4939-2864-4_304). ISBN 978-1-4939-2864-4. S2CID 3116149 (https://api.semanticscholar.org/CorpusID:3116149).
84. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (23 December 2008). "A Quantum Algorithm for the Hamiltonian NAND Tree" (https://doi.org/10.4086%2Ftoc.2008.v004a008). *Theory of Computing*. **4** (1): 169–190. doi:10.4086/toc.2008.v004a008 (https://doi.org/10.4086%2Ftoc.2008.v004a008). ISSN 1557-2862 (https://search.worldcat.org/issn/1557-2862). S2CID 8258191 (https://api.semanticscholar.org/CorpusID:8258191).
85. Williams, Colin P. (2011). *Explorations in Quantum Computing*. Springer. pp. 242–244. ISBN 978-1-84628-887-6.
86. Grover, Lov (29 May 1996). "A fast quantum mechanical algorithm for database search". arXiv:quant-ph/9605043 (https://arxiv.org/abs/quant-ph/9605043).
87. Ambainis, Ambainis (June 2004). "Quantum search algorithms". *ACM SIGACT News*. **35** (2): 22–35. arXiv:quant-ph/0504012 (https://arxiv.org/abs/quant-ph/0504012). Bibcode:2005quant.ph..4012A (https://ui.adsabs.harvard.edu/abs/2005quant.ph..4012A). doi:10.1145/992287.992296 (https://doi.org/10.1145%2F992287.992296). S2CID 11326499 (https://api.semanticscholar.org/CorpusID:11326499).
88. Rich, Steven; Gellman, Barton (1 February 2014). "NSA seeks to build quantum computer that could crack most types of encryption" (https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html). *The Washington Post*.
89. Outeiral, Carlos; Strahm, Martin; Morris, Garrett; Benjamin, Simon; Deane, Charlotte; Shi, Jiye (2021). "The prospects of quantum computing in computational molecular biology" (https://doi.org/10.1002%2Fwcms.1481). *WIREs Computational Molecular Science*. **11**. arXiv:2005.12792 (https://arxiv.org/abs/2005.12792). doi:10.1002/wcms.1481 (https://doi.org/10.1002%2Fwcms.1481). S2CID 218889377 (https://api.semanticscholar.org/CorpusID:218889377).
90. Biamonte, Jacob; Wittek, Peter; Pancotti, Nicola; Rebentrost, Patrick; Wiebe, Nathan; Lloyd, Seth (September 2017). "Quantum machine learning". *Nature*. **549** (7671): 195–202. arXiv:1611.09347 (https://arxiv.org/abs/1611.09347). Bibcode:2017Natur.549..195B (https://ui.adsabs.harvard.edu/abs/2017Natur.549..195B). doi:10.1038/nature23474 (https://doi.org/10.1038%2Fnature23474). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 28905917 (https://pubmed.ncbi.nlm.nih.gov/28905917). S2CID 64536201 (https://api.semanticscholar.org/CorpusID:64536201).
91. Harrow, Aram; Hassidim, Avinatan; Lloyd, Seth (2009). "Quantum algorithm for solving linear systems of equations". *Physical Review Letters*. **103** (15): 150502. arXiv:0811.3171 (https://arxiv.org/abs/0811.3171). Bibcode:2009PhRvL.103o0502H (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103o0502H). doi:10.1103/PhysRevLett.103.150502 (https://doi.org/10.1103%2FPhysRevLett.103.150502). PMID 19905613 (https://pubmed.ncbi.nlm.nih.gov/19905613). S2CID 5187993 (https://api.semanticscholar.org/CorpusID:5187993).

92. Benedetti, Marcello; Realpe-Gómez, John; Biswas, Rupak; Perdomo-Ortiz, Alejandro (9 August 2016). "Estimation of effective temperatures in quantum annealers for sampling applications: A case study with possible applications in deep learning" (https://doi.org/10.1103%2FPhysRevA.94.022308). *Physical Review A*. **94** (2): 022308. arXiv:1510.07611 (https://arxiv.org/abs/1510.07611). Bibcode:2016PhRvA..94b2308B (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94b2308B). doi:10.1103/PhysRevA.94.022308 (https://doi.org/10.1103%2FPhysRevA.94.022308).
93. Ajagekar, Akshay; You, Fengqi (5 December 2020). "Quantum computing assisted deep learning for fault detection and diagnosis in industrial process systems". *Computers & Chemical Engineering*. **143**: 107119. arXiv:2003.00264 (https://arxiv.org/abs/2003.00264). doi:10.1016/j.compchemeng.2020.107119 (https://doi.org/10.1016%2Fj.compchemeng.2020.107119). ISSN 0098-1354 (https://search.worldcat.org/issn/0098-1354). S2CID 211678230 (https://api.semanticscholar.org/CorpusID:211678230).
94. Ajagekar, Akshay; You, Fengqi (1 December 2021). "Quantum computing based hybrid deep learning for fault diagnosis in electrical power systems" (https://doi.org/10.1016%2Fj.apenergy.2021.117628). *Applied Energy*. **303**: 117628. Bibcode:2021ApEn..30317628A (https://ui.adsabs.harvard.edu/abs/2021ApEn..30317628A). doi:10.1016/j.apenergy.2021.117628 (https://doi.org/10.1016%2Fj.apenergy.2021.117628). ISSN 0306-2619 (https://search.worldcat.org/issn/0306-2619).
95. Gao, Xun; Anschuetz, Eric R.; Wang, Sheng-Tao; Cirac, J. Ignacio; Lukin, Mikhail D. (2022). "Enhancing Generative Models via Quantum Correlations". *Physical Review X*. **12** (2): 021037. arXiv:2101.08354 (https://arxiv.org/abs/2101.08354). Bibcode:2022PhRvX..12b1037G (https://ui.adsabs.harvard.edu/abs/2022PhRvX..12b1037G). doi:10.1103/PhysRevX.12.021037 (https://doi.org/10.1103%2FPhysRevX.12.021037). S2CID 231662294 (https://api.semanticscholar.org/CorpusID:231662294).
96. Li, Junde; Topaloglu, Rasit; Ghosh, Swaroop (9 January 2021). "Quantum Generative Models for Small Molecule Drug Discovery". arXiv:2101.03438 (https://arxiv.org/abs/2101.03438) [cs.ET (https://arxiv.org/archive/cs.ET)].
97. Brooks, Michael (24 May 2023). "Quantum computers: what are they good for?" (https://doi.org/10.1038%2Fd41586-023-01692-9). *Nature*. **617** (7962): S1–S3. Bibcode:2023Natur.617S...1B (https://ui.adsabs.harvard.edu/abs/2023Natur.617S...1B). doi:10.1038/d41586-023-01692-9 (https://doi.org/10.1038%2Fd41586-023-01692-9). PMID 37225885 (https://pubmed.ncbi.nlm.nih.gov/37225885). S2CID 258847001 (https://api.semanticscholar.org/CorpusID:258847001).
98. Torsten Hoefler; Thomas Häner; Matthias Troyer (May 2023). "Disentangling Hype from Practicality: On Realistically Achieving Quantum Advantage" (https://m-cacm.acm.org/magazines/2023/5/272276-disentangling-hype-from-practicality-on-realistically-achieving-quantum-advantage/fulltext). Communications of the ACM.
99. Dyakonov, Mikhail (15 November 2018). "The Case Against Quantum Computing" (https://spectrum.ieee.org/the-case-against-quantum-computing). *IEEE Spectrum*.
100. DiVincenzo, David P. (13 April 2000). "The Physical Implementation of Quantum Computation". *Fortschritte der Physik*. **48** (9–11): 771–783. arXiv:quant-ph/0002077 (https://arxiv.org/abs/quant-ph/0002077). Bibcode:2000ForPh..48..771D (https://ui.adsabs.harvard.edu/abs/2000ForPh..48..771D). doi:10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E (https://doi.org/10.1002%2F1521-3978%28200009%2948%3A9%2F11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E). S2CID 15439711 (https://api.semanticscholar.org/CorpusID:15439711).
101. Giles, Martin (17 January 2019). "We'd have more quantum computers if it weren't so hard to find the damn cables" (https://www.technologyreview.com/s/612760/quantum-computers-component-shortage/). MIT Technology Review. Retrieved 17 May 2021.

102. Pauka SJ, Das K, Kalra B, Moini A, Yang Y, Trainer M, Bousquet A, Cantaloube C, Dick N, Gardner GC, Manfra MJ, Reilly DJ (2021). "A cryogenic CMOS chip for generating control signals for multiple qubits" (https://www.nature.com/articles/s41928-020-00528-y). *Nature Electronics*. **4** (4): 64–70. arXiv:1912.01299 (https://arxiv.org/abs/1912.01299). doi:10.1038/s41928-020-00528-y (https://doi.org/10.1038%2Fs41928-020-00528-y). S2CID 231715555 (https://api.semanticscholar.org/CorpusID:231715555).
103. DiVincenzo, David P. (1995). "Quantum Computation". *Science*. **270** (5234): 255–261. Bibcode:1995Sci...270..255D (https://ui.adsabs.harvard.edu/abs/1995Sci...270..255D). CiteSeerX 10.1.1.242.2165 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.242.2165). doi:10.1126/science.270.5234.255 (https://doi.org/10.1126%2Fscience.270.5234.255). S2CID 220110562 (https://api.semanticscholar.org/CorpusID:220110562).
104. Zu, H.; Dai, W.; de Waele, A.T.A.M. (2022). "Development of Dilution refrigerators – A review". *Cryogenics*. **121**. doi:10.1016/j.cryogenics.2021.103390 (https://doi.org/10.1016%2Fj.cryogenics.2021.103390). ISSN 0011-2275 (https://search.worldcat.org/issn/0011-2275). S2CID 244005391 (https://api.semanticscholar.org/CorpusID:244005391).
105. Jones, Nicola (19 June 2013). "Computing: The quantum company" (https://doi.org/10.1038%2F498286a). *Nature*. **498** (7454): 286–288. Bibcode:2013Natur.498..286J (https://ui.adsabs.harvard.edu/abs/2013Natur.498..286J). doi:10.1038/498286a (https://doi.org/10.1038%2F498286a). PMID 23783610 (https://pubmed.ncbi.nlm.nih.gov/23783610).
106. Vepsäläinen, Antti P.; Karamlou, Amir H.; Orrell, John L.; Dogra, Akshunna S.; Loer, Ben; et al. (August 2020). "Impact of ionizing radiation on superconducting qubit coherence" (https://www.nature.com/articles/s41586-020-2619-8). *Nature*. **584** (7822): 551–556. arXiv:2001.09190 (https://arxiv.org/abs/2001.09190). Bibcode:2020Natur.584..551V (https://ui.adsabs.harvard.edu/abs/2020Natur.584..551V). doi:10.1038/s41586-020-2619-8 (https://doi.org/10.1038%2Fs41586-020-2619-8). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 32848227 (https://pubmed.ncbi.nlm.nih.gov/32848227). S2CID 210920566 (https://api.semanticscholar.org/CorpusID:210920566).
107. Amy, Matthew; Matteo, Olivia; Gheorghiu, Vlad; Mosca, Michele; Parent, Alex; Schanck, John (30 November 2016). "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3". arXiv:1603.09383 (https://arxiv.org/abs/1603.09383) [quant-ph (https://arxiv.org/archive/quant-ph)].
108. Dyakonov, M. I. (14 October 2006). S. Luryi; Xu, J.; Zaslavsky, A. (eds.). "Is Fault-Tolerant Quantum Computation Really Possible?". *Future Trends in Microelectronics. Up the Nano Creek*: 4–18. arXiv:quant-ph/0610117 (https://arxiv.org/abs/quant-ph/0610117). Bibcode:2006quant.ph.10117D (https://ui.adsabs.harvard.edu/abs/2006quant.ph.10117D).
109. Ahsan, Muhammad (2015). *Architecture Framework for Trapped-ion Quantum Computer based on Performance Simulation Tool* (http://worldcat.org/oclc/923881411). OCLC 923881411 (https://search.worldcat.org/oclc/923881411).
110. Ahsan, Muhammad; Meter, Rodney Van; Kim, Jungsang (28 December 2016). "Designing a Million-Qubit Quantum Computer Using a Resource Performance Simulator" (https://doi.org/10.1145%2F2830570). *ACM Journal on Emerging Technologies in Computing Systems*. **12** (4): 39:1–39:25. arXiv:1512.00796 (https://arxiv.org/abs/1512.00796). doi:10.1145/2830570 (https://doi.org/10.1145%2F2830570). ISSN 1550-4832 (https://search.worldcat.org/issn/1550-4832). S2CID 1258374 (https://api.semanticscholar.org/CorpusID:1258374).
111. Gidney, Craig; Ekerå, Martin (15 April 2021). "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". *Quantum*. **5**: 433. arXiv:1905.09749 (https://arxiv.org/abs/1905.09749). Bibcode:2021Quant...5..433G (https://ui.adsabs.harvard.edu/abs/2021Quant...5..433G). doi:10.22331/q-2021-04-15-433 (https://doi.org/10.22331%2Fq-2021-04-15-433). ISSN 2521-327X (https://search.worldcat.org/issn/2521-327X). S2CID 162183806 (https://api.semanticscholar.org/CorpusID:162183806).

112. Freedman, Michael H.; Kitaev, Alexei; Larsen, Michael J.; Wang, Zhenghan (2003). "Topological quantum computation". *Bulletin of the American Mathematical Society*. **40** (1): 31–38. arXiv:quant-ph/0101025 (https://arxiv.org/abs/quant-ph/0101025). doi:10.1090/S0273-0979-02-00964-3 (https://doi.org/10.1090%2FS0273-0979-02-00964-3). MR 1943131 (https://mathscinet.ams.org/mathscinet-getitem?mr=1943131).
113. Monroe, Don (1 October 2008). "Anyons: The breakthrough quantum computing needs?" (https://www.newscientist.com/channel/fundamentals/mg20026761.700-anyons-the-breakthrough-quantum-computing-needs.html). *New Scientist*.
114. Preskill, John (26 March 2012). "Quantum computing and the entanglement frontier". arXiv:1203.5813 (https://arxiv.org/abs/1203.5813) [quant-ph (https://arxiv.org/archive/quant-ph)].
115. Preskill, John (6 August 2018). "Quantum Computing in the NISQ era and beyond" (https://doi.org/10.22331%2Fq-2018-08-06-79). *Quantum*. **2**: 79. arXiv:1801.00862 (https://arxiv.org/abs/1801.00862). Bibcode:2018Quant...2...79P (https://ui.adsabs.harvard.edu/abs/2018Quant...2...79P). doi:10.22331/q-2018-08-06-79 (https://doi.org/10.22331%2Fq-2018-08-06-79).
116. Boixo, Sergio; Isakov, Sergei V.; Smelyanskiy, Vadim N.; Babbush, Ryan; Ding, Nan; et al. (2018). "Characterizing Quantum Supremacy in Near-Term Devices". *Nature Physics*. **14** (6): 595–600. arXiv:1608.00263 (https://arxiv.org/abs/1608.00263). Bibcode:2018NatPh..14..595B (https://ui.adsabs.harvard.edu/abs/2018NatPh..14..595B). doi:10.1038/s41567-018-0124-x (https://doi.org/10.1038%2Fs41567-018-0124-x). S2CID 4167494 (https://api.semanticscholar.org/CorpusID:4167494).
117. Savage, Neil (5 July 2017). "Quantum Computers Compete for "Supremacy" " (https://www.scientificamerican.com/article/quantum-computers-compete-for-supremacy/). *Scientific American*.
118. Giles, Martin (20 September 2019). "Google researchers have reportedly achieved 'quantum supremacy' " (https://www.technologyreview.com/f/614416/google-researchers-have-reportedly-achieved-quantum-supremacy/). *MIT Technology Review*. Retrieved 15 May 2020.
119. Tavares, Frank (23 October 2019). "Google and NASA Achieve Quantum Supremacy" (http://www.nasa.gov/feature/ames/quantum-supremacy). *NASA*. Retrieved 16 November 2021.
120. Pednault, Edwin; Gunnels, John A.; Nannicini, Giacomo; Horesh, Lior; Wisnieff, Robert (22 October 2019). "Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits". arXiv:1910.09534 (https://arxiv.org/abs/1910.09534) [quant-ph (https://arxiv.org/archive/quant-ph)].
121. Cho, Adrian (23 October 2019). "IBM casts doubt on Google's claims of quantum supremacy" (https://www.science.org/content/article/ibm-casts-doubt-googles-claims-quantum-supremacy). *Science*. doi:10.1126/science.aaz6080 (https://doi.org/10.1126%2Fscience.aaz6080). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). S2CID 211982610 (https://api.semanticscholar.org/CorpusID:211982610).
122. Liu, Yong (Alexander); Liu, Xin (Lucy); Li, Fang (Nancy); Fu, Haohuan; Yang, Yuling; et al. (14 November 2021). "Closing the "quantum supremacy" gap". *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. SC '21. New York, New York: Association for Computing Machinery. pp. 1–12. arXiv:2110.14502 (https://arxiv.org/abs/2110.14502). doi:10.1145/3458817.3487399 (https://doi.org/10.1145%2F3458817.3487399). ISBN 978-1-4503-8442-1. S2CID 239036985 (https://api.semanticscholar.org/CorpusID:239036985).

123. Bulmer, Jacob F. F.; Bell, Bryn A.; Chadwick, Rachel S.; Jones, Alex E.; Moise, Diana; et al. (28 January 2022). "The boundary for quantum advantage in Gaussian boson sampling" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8791606). *Science Advances*. **8** (4): eabl9236. arXiv:2108.01622 (https://arxiv.org/abs/2108.01622). Bibcode:2022SciA....8.9236B (https://ui.adsabs.harvard.edu/abs/2022SciA....8.9236B). doi:10.1126/sciadv.abl9236 (https://doi.org/10.1126%2Fsciadv.abl9236). ISSN 2375-2548 (https://search.worldcat.org/issn/2375-2548). PMC 8791606 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8791606). PMID 35080972 (https://pubmed.ncbi.nlm.nih.gov/35080972).
124. McCormick, Katie (10 February 2022). "Race Not Over Between Classical and Quantum Computers" (https://physics.aps.org/articles/v15/19). *Physics*. **15**: 19. Bibcode:2022PhyOJ..15...19M (https://ui.adsabs.harvard.edu/abs/2022PhyOJ..15...19M). doi:10.1103/Physics.15.19 (https://doi.org/10.1103%2FPhysics.15.19). S2CID 246910085 (https://api.semanticscholar.org/CorpusID:246910085).
125. Pan, Feng; Chen, Keyang; Zhang, Pan (2022). "Solving the Sampling Problem of the Sycamore Quantum Circuits". *Physical Review Letters*. **129** (9): 090502. arXiv:2111.03011 (https://arxiv.org/abs/2111.03011). Bibcode:2022PhRvL.129i0502P (https://ui.adsabs.harvard.edu/abs/2022PhRvL.129i0502P). doi:10.1103/PhysRevLett.129.090502 (https://doi.org/10.1103%2FPhysRevLett.129.090502). PMID 36083655 (https://pubmed.ncbi.nlm.nih.gov/36083655). S2CID 251755796 (https://api.semanticscholar.org/CorpusID:251755796).
126. Cho, Adrian (2 August 2022). "Ordinary computers can beat Google's quantum computer after all" (https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all). *Science*. **377**. doi:10.1126/science.ade2364 (https://doi.org/10.1126%2Fscience.ade2364).
127. "Google's 'quantum supremacy' usurped by researchers using ordinary supercomputer" (https://techcrunch.com/2022/08/05/googles-quantum-supremacy-usurped-by-researchers-using-ordinary-supercomputer/). *TechCrunch*. 5 August 2022. Retrieved 7 August 2022.
128. Ball, Philip (3 December 2020). "Physicists in China challenge Google's 'quantum advantage' ". *Nature*. **588** (7838): 380. Bibcode:2020Natur.588..380B (https://ui.adsabs.harvard.edu/abs/2020Natur.588..380B). doi:10.1038/d41586-020-03434-7 (https://doi.org/10.1038%2Fd41586-020-03434-7). PMID 33273711 (https://pubmed.ncbi.nlm.nih.gov/33273711). S2CID 227282052 (https://api.semanticscholar.org/CorpusID:227282052).
129. Garisto, Daniel. "Light-based Quantum Computer Exceeds Fastest Classical Supercomputers" (https://www.scientificamerican.com/article/light-based-quantum-computer-exceeds-fastest-classical-supercomputers/). *Scientific American*. Retrieved 7 December 2020.
130. Conover, Emily (3 December 2020). "The new light-based quantum computer Jiuzhang has achieved quantum supremacy" (https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy). *Science News*. Retrieved 7 December 2020.
131. Zhong, Han-Sen; Wang, Hui; Deng, Yu-Hao; Chen, Ming-Cheng; Peng, Li-Chao; et al. (3 December 2020). "Quantum computational advantage using photons". *Science*. **370** (6523): 1460–1463. arXiv:2012.01625 (https://arxiv.org/abs/2012.01625). Bibcode:2020Sci...370.1460Z (https://ui.adsabs.harvard.edu/abs/2020Sci...370.1460Z). doi:10.1126/science.abe8770 (https://doi.org/10.1126%2Fscience.abe8770). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33273064 (https://pubmed.ncbi.nlm.nih.gov/33273064). S2CID 227254333 (https://api.semanticscholar.org/CorpusID:227254333).
132. Roberson, Tara M. (21 May 2020). "{{subst:title case|Can hype be a force for good?}}" (https://doi.org/10.1177%2F0963662520923109). *Public Understanding of Science*. **29** (5): 544–552. doi:10.1177/0963662520923109 (https://doi.org/10.1177%2F0963662520923109). ISSN 0963-6625 (https://search.worldcat.org/issn/0963-6625). PMID 32438851 (https://pubmed.ncbi.nlm.nih.gov/32438851). S2CID 218831653 (https://api.semanticscholar.org/CorpusID:218831653).

133. Cavaliere, Fabio; Mattsson, John; Smeets, Ben (September 2020). "The security implications of quantum cryptography and quantum computing" (http://www.magonlinelibrary.com/doi/10.1016/S1353-4858%2820%2930105-7). *Network Security*. **2020** (9): 9–15. doi:10.1016/S1353-4858(20)30105-7 (https://doi.org/10.1016%2FS1353-4858%2820%2930105-7). ISSN 1353-4858 (https://search.worldcat.org/issn/1353-4858). S2CID 222349414 (https://api.semanticscholar.org/CorpusID:222349414).
134. Liu, Yong; Chen, Yaojian; Guo, Chu; Song, Jiawei; Shi, Xinmin; Gan, Lin; Wu, Wenzhao; Wu, Wei; Fu, Haohuan; Liu, Xin; Chen, Dexun; Zhao, Zhifeng; Yang, Guangwen; Gao, Jiangang (16 January 2024). "Verifying Quantum Advantage Experiments with Multiple Amplitude Tensor Network Contraction" (https://link.aps.org/doi/10.1103/PhysRevLett.132.030601). *Physical Review Letters*. **132** (3): 030601. arXiv:2212.04749 (https://arxiv.org/abs/2212.04749). Bibcode:2024PhRvL.132c0601L (https://ui.adsabs.harvard.edu/abs/2024PhRvL.132c0601L). doi:10.1103/PhysRevLett.132.030601 (https://doi.org/10.1103%2FPhysRevLett.132.030601). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 38307065 (https://pubmed.ncbi.nlm.nih.gov/38307065).
135. Monroe, Don (December 2022). "Quantum Computers and the Universe" (https://m-cacm.acm.org/magazines/2022/12/266916-quantum-computers-and-the-universe/fulltext). Communications of the ACM.
136. Swayne, Matt (20 June 2023). "PsiQuantum Sees 700x Reduction in Computational Resource Requirements to Break Elliptic Curve Cryptography With a Fault Tolerant Quantum Computer" (https://thequantuminsider.com/2023/06/20/psiquantum-sees-700x-reduction-in-computational-resource-requirements-to-break-elliptic-curve-cryptography-with-a-fault-tolerant-quantum-computer/). *The Quanrum Insider*.
137. Unruh, Bill (1995). "Maintaining coherence in Quantum Computers". *Physical Review A*. **51** (2): 992–997. arXiv:hep-th/9406058 (https://arxiv.org/abs/hep-th/9406058). Bibcode:1995PhRvA..51..992U (https://ui.adsabs.harvard.edu/abs/1995PhRvA..51..992U). doi:10.1103/PhysRevA.51.992 (https://doi.org/10.1103%2FPhysRevA.51.992). PMID 9911677 (https://pubmed.ncbi.nlm.nih.gov/9911677). S2CID 13980886 (https://api.semanticscholar.org/CorpusID:13980886).
138. Davies, Paul (6 March 2007). "The implications of a holographic universe for quantum information science and the nature of physical law". arXiv:quant-ph/0703041 (https://arxiv.org/abs/quant-ph/0703041).
139. Regan, K. W. (23 April 2016). "Quantum Supremacy and Complexity" (https://rjlipton.wordpress.com/2016/04/22/quantum-supremacy-and-complexity/). *Gödel's Lost Letter and P=NP*.
140. Kalai, Gil (May 2016). "The Quantum Computer Puzzle" (https://www.ams.org/journals/notices/201605/rnoti-p508.pdf) (PDF). *Notices of the AMS*. **63** (5): 508–516.
141. Rinott, Yosef; Shoham, Tomer; Kalai, Gil (13 July 2021). "Statistical Aspects of the Quantum Supremacy Demonstration". arXiv:2008.05177 (https://arxiv.org/abs/2008.05177) [quant-ph (https://arxiv.org/archive/quant-ph)].
142. Dyakonov, Mikhail (15 November 2018). "The Case Against Quantum Computing" (https://spectrum.ieee.org/the-case-against-quantum-computing). *IEEE Spectrum*. Retrieved 3 December 2019.
143. Dyakonov, Mikhail (24 March 2020). *Will We Ever Have a Quantum Computer?* (https://www.springer.com/gp/book/9783030420185). Springer. ISBN 9783030420185. Retrieved 22 May 2020.
144. Tacchino, Francesco; Chiesa, Alessandro; Carretta, Stefano; Gerace, Dario (19 December 2019). "Quantum Computers as Universal Quantum Simulators: State-of-the-Art and Perspectives" (https://onlinelibrary.wiley.com/doi/10.1002/qute.201900052). *Advanced Quantum Technologies*. **3** (3): 1900052. arXiv:1907.03505 (https://arxiv.org/abs/1907.03505). doi:10.1002/qute.201900052 (https://doi.org/10.1002%2Fqute.201900052). ISSN 2511-9044 (https://search.worldcat.org/issn/2511-9044). S2CID 195833616 (https://api.semanticscholar.org/CorpusID:195833616).

145. Grumbling & Horowitz 2019, p. 127.
146. Grumbling & Horowitz 2019, p. 114.
147. Grumbling & Horowitz 2019, p. 119.
148. Grumbling & Horowitz 2019, p. 126.
149. Nielsen & Chuang 2010, p. 29.
150. Nielsen & Chuang 2010, p. 126.
151. Nielsen & Chuang 2010, p. 41.
152. Nielsen & Chuang 2010, p. 201.
153. Bernstein, Ethan; Vazirani, Umesh (1997). "Quantum Complexity Theory" (http://www.cs.berkeley.edu/~vazirani/bv.ps). *SIAM Journal on Computing*. **26** (5): 1411–1473. CiteSeerX 10.1.1.144.7852 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.7852). doi:10.1137/S0097539796300921 (https://doi.org/10.1137%2FS0097539796300921).

Sources

- Aaronson, Scott (2013). *Quantum Computing Since Democritus*. Cambridge University Press. doi:10.1017/CBO9780511979309 (https://doi.org/10.1017%2FCBO9780511979309). ISBN 978-0-521-19956-8. OCLC 829706638 (https://search.worldcat.org/oclc/829706638).
- Grumbling, Emily; Horowitz, Mark, eds. (2019). *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press. doi:10.17226/25196 (https://doi.org/10.17226%2F25196). ISBN 978-0-309-47970-7. OCLC 1091904777 (https://search.worldcat.org/oclc/1091904777). S2CID 125635007 (https://api.semanticscholar.org/CorpusID:125635007).
- Mermin, N. David (2007). *Quantum Computer Science: An Introduction*. doi:10.1017/CBO9780511813870 (https://doi.org/10.1017%2FCBO9780511813870). ISBN 978-0-511-34258-5. OCLC 422727925 (https://search.worldcat.org/oclc/422727925).
- Nielsen, Michael; Chuang, Isaac (2010). *Quantum Computation and Quantum Information* (10th anniversary ed.). doi:10.1017/CBO9780511976667 (https://doi.org/10.1017%2FCBO9780511976667). ISBN 978-0-511-99277-3. OCLC 700706156 (https://search.worldcat.org/oclc/700706156). S2CID 59717455 (https://api.semanticscholar.org/CorpusID:59717455).
- Shor, Peter W. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. Symposium on Foundations of Computer Science. Santa Fe, New Mexico: IEEE. pp. 124–134. doi:10.1109/SFCS.1994.365700 (https://doi.org/10.1109%2FSFCS.1994.365700). ISBN 978-0-8186-6580-6.

Further reading

Textbooks

- Akama, Seiki (2014). *Elements of Quantum Computing: History, Theories and Engineering Applications*. Springer. doi:10.1007/978-3-319-08284-4 (https://doi.org/10.1007%2F978-3-319-08284-4). ISBN 978-3-319-08284-4. OCLC 884786739 (https://search.worldcat.org/oclc/884786739).

- Benenti, Giuliano; Casati, Giulio; Rossini, Davide; Strini, Giuliano (2019). *Principles of Quantum Computation and Information: A Comprehensive Textbook* (2nd ed.). doi:10.1142/10909 (https://doi.org/10.1142%2F10909). ISBN 978-981-3237-23-0. OCLC 1084428655 (https://search.worldcat.org/oclc/1084428655). S2CID 62280636 (https://api.semanticscholar.org/CorpusID:62280636).
- Bernhardt, Chris (2019). *Quantum Computing for Everyone*. MIT Press. ISBN 978-0-262-35091-4. OCLC 1082867954 (https://search.worldcat.org/oclc/1082867954).
- Hidary, Jack D. (2021). *Quantum Computing: An Applied Approach* (2nd ed.). doi:10.1007/978-3-030-83274-2 (https://doi.org/10.1007%2F978-3-030-83274-2). ISBN 978-3-03-083274-2. OCLC 1272953643 (https://search.worldcat.org/oclc/1272953643). S2CID 238223274 (https://api.semanticscholar.org/CorpusID:238223274).
- Hiroshi, Imai; Masahito, Hayashi, eds. (2006). *Quantum Computation and Information: From Theory to Experiment*. Topics in Applied Physics. Vol. 102. doi:10.1007/3-540-33133-6 (https://doi.org/10.1007%2F3-540-33133-6). ISBN 978-3-540-33133-9.
- Hughes, Ciaran; Isaacson, Joshua; Perry, Anastasia; Sun, Ranbel F.; Turner, Jessica (2021). *Quantum Computing for the Quantum Curious* (https://link.springer.com/content/pdf/10.1007/978-3-030-61601-4.pdf) (PDF). doi:10.1007/978-3-030-61601-4 (https://doi.org/10.1007%2F978-3-030-61601-4). ISBN 978-3-03-061601-4. OCLC 1244536372 (https://search.worldcat.org/oclc/1244536372). S2CID 242566636 (https://api.semanticscholar.org/CorpusID:242566636).
- Jaeger, Gregg (2007). *Quantum Information: An Overview*. doi:10.1007/978-0-387-36944-0 (https://doi.org/10.1007%2F978-0-387-36944-0). ISBN 978-0-387-36944-0. OCLC 186509710 (https://search.worldcat.org/oclc/186509710).
- Johnston, Eric R.; Harrigan, Nic; Gimeno-Segovia, Mercedes (2019). *Programming Quantum Computers: Essential Algorithms and Code Samples*. O'Reilly Media, Incorporated. ISBN 978-1-4920-3968-6. OCLC 1111634190 (https://search.worldcat.org/oclc/1111634190).
- Kaye, Phillip; Laflamme, Raymond; Mosca, Michele (2007). *An Introduction to Quantum Computing*. OUP Oxford. ISBN 978-0-19-857000-4. OCLC 85896383 (https://search.worldcat.org/oclc/85896383).
- Kitaev, Alexei Yu.; Shen, Alexander H.; Vyalyi, Mikhail N. (2002). *Classical and Quantum Computation*. American Mathematical Soc. ISBN 978-0-8218-3229-5. OCLC 907358694 (https://search.worldcat.org/oclc/907358694).
- Kurgalin, Sergei; Borzunov, Sergei (2021). *Concise Guide to Quantum Computing: Algorithms, Exercises, and Implementations* (https://dx.doi.org/10.1007/978-3-030-65052-0). Springer. doi:10.1007/978-3-030-65052-0 (https://doi.org/10.1007%2F978-3-030-65052-0). ISBN 978-3-030-65052-0.
- Stolze, Joachim; Suter, Dieter (2004). *Quantum Computing: A Short Course from Theory to Experiment*. doi:10.1002/9783527617760 (https://doi.org/10.1002%2F9783527617760). ISBN 978-3-527-61776-0. OCLC 212140089 (https://search.worldcat.org/oclc/212140089).
- Susskind, Leonard; Friedman, Art (2014). *Quantum Mechanics: The Theoretical Minimum*. New York: Basic Books. ISBN 978-0-465-08061-8.
- Wichert, Andreas (2020). *Principles of Quantum Artificial Intelligence: Quantum Problem Solving and Machine Learning* (2nd ed.). doi:10.1142/11938 (https://doi.org/10.1142%2F11938). ISBN 978-981-12-2431-7. OCLC 1178715016 (https://search.worldcat.org/oclc/1178715016). S2CID 225498497 (https://api.semanticscholar.org/CorpusID:225498497).
- Wong, Thomas (2022). *Introduction to Classical and Quantum Computing* (https://web.archive.org/web/20220129214631/http://www.thomaswong.net/introduction-to-classical-and-quantum-computing-1e.pdf) (PDF). Rooted Grove. ISBN 979-8-9855931-0-5. OCLC 1308951401 (https://search.worldcat.org/oclc/1308951401). Archived from the original (http://www.thomaswong.net/introduction-to-classical-and-quantum-computing-1e.pdf) (PDF) on 29 January 2022. Retrieved 6 February 2022.

- Zeng, Bei; Chen, Xie; Zhou, Duan-Lu; Wen, Xiao-Gang (2019). *Quantum Information Meets Quantum Matter*. arXiv:1508.02595 (https://arxiv.org/abs/1508.02595). doi:10.1007/978-1-4939-9084-9 (https://doi.org/10.1007%2F978-1-4939-9084-9). ISBN 978-1-4939-9084-9. OCLC 1091358969 (https://search.worldcat.org/oclc/1091358969). S2CID 118528258 (https://api.semanticscholar.org/CorpusID:118528258).

Academic papers

- Abbot, Derek; Doering, Charles R.; Caves, Carlton M.; Lidar, Daniel M.; Brandt, Howard E.; et al. (2003). "Dreams versus Reality: Plenary Debate Session on Quantum Computing". *Quantum Information Processing*. **2** (6): 449–472. arXiv:quant-ph/0310130 (https://arxiv.org/abs/quant-ph/0310130). Bibcode:2003QuIP....2..449A (https://ui.adsabs.harvard.edu/abs/2003QuIP....2..449A). doi:10.1023/B:QINP.0000042203.24782.9a (https://doi.org/10.1023%2FB%3AQINP.0000042203.24782.9a). hdl:2027.42/45526 (https://hdl.handle.net/2027.42%2F45526). S2CID 34885835 (https://api.semanticscholar.org/CorpusID:34885835).
- Berthiaume, Andre (1 December 1998). "Quantum Computation". *Solution Manual for Quantum Mechanics*. pp. 233–234. doi:10.1142/9789814541893_0016 (https://doi.org/10.1142%2F9789814541893_0016). ISBN 978-981-4541-88-6. S2CID 128255429 (https://api.semanticscholar.org/CorpusID:128255429) – via Semantic Scholar.
- DiVincenzo, David P. (2000). "The Physical Implementation of Quantum Computation". *Fortschritte der Physik*. **48** (9–11): 771–783. arXiv:quant-ph/0002077 (https://arxiv.org/abs/quant-ph/0002077). Bibcode:2000ForPh..48..771D (https://ui.adsabs.harvard.edu/abs/2000ForPh..48..771D). doi:10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E (https://doi.org/10.1002%2F1521-3978%28200009%2948%3A9%2F11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E). S2CID 15439711 (https://api.semanticscholar.org/CorpusID:15439711).
- DiVincenzo, David P. (1995). "Quantum Computation". *Science*. **270** (5234): 255–261. Bibcode:1995Sci...270..255D (https://ui.adsabs.harvard.edu/abs/1995Sci...270..255D). CiteSeerX 10.1.1.242.2165 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.242.2165). doi:10.1126/science.270.5234.255 (https://doi.org/10.1126%2Fscience.270.5234.255). S2CID 220110562 (https://api.semanticscholar.org/CorpusID:220110562). Table 1 lists switching and dephasing times for various systems.
- Feynman, Richard (1982). "Simulating physics with computers". *International Journal of Theoretical Physics*. **21** (6–7): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). CiteSeerX 10.1.1.45.9310 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9310). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445).
- Jeutner, Valentin (2021). "The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers" (https://lup.lub.lu.se/record/e034e7b7-d17c-4863-9cee-7e654f97225b). *Morals & Machines*. **1** (1): 52–59. doi:10.5771/2747-5174-2021-1-52 (https://doi.org/10.5771%2F2747-5174-2021-1-52). S2CID 236664155 (https://api.semanticscholar.org/CorpusID:236664155).
- Krantz, P.; Kjaergaard, M.; Yan, F.; Orlando, T. P.; Gustavsson, S.; Oliver, W. D. (17 June 2019). "A Quantum Engineer's Guide to Superconducting Qubits". *Applied Physics Reviews*. **6** (2): 021318. arXiv:1904.06560 (https://arxiv.org/abs/1904.06560). Bibcode:2019ApPRv...6b1318K (https://ui.adsabs.harvard.edu/abs/2019ApPRv...6b1318K). doi:10.1063/1.5089550 (https://doi.org/10.1063%2F1.5089550). ISSN 1931-9401 (https://search.worldcat.org/issn/1931-9401). S2CID 119104251 (https://api.semanticscholar.org/CorpusID:119104251).
- Mitchell, Ian (1998). "Computing Power into the 21st Century: Moore's Law and Beyond" (http://citeseer.ist.psu.edu/mitchell98computing.html).

- Simon, Daniel R. (1994). "On the Power of Quantum Computation" (http://citeseer.ist.psu.edu/simon94power.html). Institute of Electrical and Electronics Engineers Computer Society Press.

External links

- Media related to Quantum computer at Wikimedia Commons
- Learning materials related to Quantum computing at Wikiversity
- Stanford Encyclopedia of Philosophy: "Quantum Computing (http://plato.stanford.edu/entries/qt-quantcomp/)" by Amit Hagar and Michael E. Cuffaro.
- "Quantum computation, theory of" (https://www.encyclopediaofmath.org/index.php?title=Quantum_computation,_theory_of), *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]
- Quantum computing for the very curious (https://quantum.country/qcvc) by Andy Matuschak and Michael Nielsen

Lectures

- Quantum computing for the determined (https://www.youtube.com/playlist?list=PL1826E60FD05B44E4) – 22 video lectures by Michael Nielsen
- Video Lectures (http://www.quiprocone.org/Protected/DD_lectures.htm) by David Deutsch
- Lectures at the Institut Henri Poincaré (slides and videos) (https://web.archive.org/web/20160303183533/http://www.quantware.ups-tlse.fr/IHP2006/)
- Online lecture on An Introduction to Quantum Computing, Edward Gerjuoy (2008) (https://web.archive.org/web/20130901004919/http://nanohub.org/resources/4778)
- Lomonaco, Sam. Four Lectures on Quantum Computing given at Oxford University in July 2006 (http://www.csee.umbc.edu/~lomonaco/Lectures.html#OxfordLectures)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_computing&oldid=1245589848"

WIKIPEDIA
The Free Encyclopedia

Timeline of quantum computing and communication

This is a **timeline of quantum computing**.

1960s

1968

- Stephen Wiesner invents conjugate coding (published in ACM SIGACT News 15(1): 78–88).[1]

1970s

1970

- James Park articulates the no-cloning theorem.[2]

1973

- Alexander Holevo publishes a paper showing that *n* qubits can carry more than *n* classical bits of information, but at most *n* classical bits are accessible (a result known as "Holevo's theorem" or "Holevo's bound").
- Charles H. Bennett shows that computation can be done reversibly.[3]

1975

- R. P. Poplavskii publishes "Thermodynamical models of information processing" (in Russian)[4] which shows the computational infeasibility of simulating quantum systems on classical computers, due to the superposition principle.

1976

- Roman Stanisław Ingarden, a Polish mathematical physicist, publishes the paper "Quantum Information Theory" in Reports on Mathematical Physics, vol. 10, pp. 43–72, 1976 (The paper was submitted in 1975). It is one of the first attempts at creating a quantum information theory, showing that Shannon information theory cannot directly be generalized to the quantum case, but rather that it is possible to construct a quantum information theory, which is a generalization of Shannon's theory, within the formalism of a generalized

quantum mechanics of open systems and a generalized concept of observables (the so-called semi-observables).

1980s

1980

- Paul Benioff describes the first quantum mechanical model of a computer. In this work, Benioff showed that a computer could operate under the laws of quantum mechanics by describing a Schrödinger equation description of Turing machines, laying a foundation for further work in quantum computing. The paper[5] was submitted in June 1979 and published in April 1980.
- Yuri Manin briefly motivates the idea of quantum computing.[6]
- Tommaso Toffoli introduces the reversible Toffoli gate,[7] which (together with initialized ancilla bits) is functionally complete for reversible classical computation.

1981

- At the first Conference on the Physics of Computation, held at the Massachusetts Institute of Technology (MIT) in May,[8] Paul Benioff and Richard Feynman give talks on quantum computing. Benioff's built on his earlier 1980 work showing that a computer can operate under the laws of quantum mechanics. The talk was titled “Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines”.[9] In Feynman's talk, he observed that it appeared to be impossible to efficiently simulate an evolution of a quantum system on a classical computer, and he proposed a basic model for a quantum computer.[10]

1982

- Paul Benioff further develops his original model of a quantum mechanical Turing machine.[11]
- William Wootters and Wojciech Zurek,[12] and independently Dennis Dieks[13] rediscover the no-cloning theorem of James Park.

1984

- Charles Bennett and Gilles Brassard employ Wiesner's conjugate coding for distribution of cryptographic keys.[14]

1985

- David Deutsch, at the University of Oxford, describes the first universal quantum computer. Just as a Universal Turing machine can simulate any other Turing machine efficiently (Church–Turing thesis), so the universal quantum computer is able to simulate any other quantum computer with at most a polynomial slowdown.

- Asher Peres points out the need for quantum error correction schemes and discusses a repetition code for amplitude errors.[15]

1988

- Yoshihisa Yamamoto and K. Igeta propose the first physical realization of a quantum computer, including Feynman's CNOT gate.[16] Their approach uses atoms and photons and is the progenitor of modern quantum computing and networking protocols using photons to transmit qubits and atoms to perform two-qubit operations.

1989

- Gerard J. Milburn proposes a quantum-optical realization of a Fredkin gate.[17]
- Bikas K. Chakrabarti & collaborators from Saha Institute of Nuclear Physics, Kolkata, India, propose that quantum fluctuations could help explore rugged energy landscapes by escaping from local minima of glassy systems having tall but thin barriers by tunneling (instead of climbing over using thermal excitations), suggesting the effectiveness of quantum annealing over classical simulated annealing.[18][19]

1990s

1991

- Artur Ekert at the University of Oxford, proposes entanglement-based secure communication.[20]

1992

- David Deutsch and Richard Jozsa propose a computational problem that can be solved efficiently with the deterministic Deutsch–Jozsa algorithm on a quantum computer, but for which no deterministic classical algorithm is possible. This was perhaps the earliest result in the computational complexity of quantum computers, proving that they were capable of performing *some* well-defined computational task more efficiently than any classical computer.
- Ethan Bernstein and Umesh Vazirani propose the Bernstein–Vazirani algorithm. It is a restricted version of the Deutsch–Jozsa algorithm where instead of distinguishing between two different classes of functions, it tries to learn a string encoded in a function. The Bernstein–Vazirani algorithm was designed to prove an oracle separation between complexity classes BQP and BPP.
- Research groups at Max Planck Institute of Quantum Optics (Garching)[21][22] and shortly after at NIST (Boulder)[23] experimentally realize the first crystallized strings of laser-cooled ions. Linear ion crystals constitute the qubit basis for most quantum computing and simulation experiments with trapped ions.

1993

- Dan Simon, at Université de Montréal, invent an oracle problem, Simon's problem, for which a quantum computer would be exponentially faster than a conventional computer. This

algorithm introduces the main ideas which were then developed in Peter Shor's factorization algorithm.

1994

- Peter Shor, at AT&T's Bell Labs in New Jersey, publishes Shor's algorithm. It would allow a quantum computer to factor large integers quickly. It solves both the factoring problem and the discrete log problem. The algorithm can theoretically break many of the cryptosystems in use today. Its invention sparked a tremendous interest in quantum computers.
- The first United States Government workshop on quantum computing is organized by NIST in Gaithersburg, Maryland, in autumn.
- Isaac Chuang and Yoshihisa Yamamoto propose a quantum-optical realization of a quantum computer to implement Deutsch's algorithm.[24] Their work introduced dual-rail encoding for photonic qubits.
- In December, Ignacio Cirac, at University of Castilla-La Mancha at Ciudad Real, and Peter Zoller at the University of Innsbruck propose an experimental realization of the controlled-NOT gate with cold trapped ions.

1995

- The first United States Department of Defense workshop on quantum computing and quantum cryptography is organized by United States Army physicists Charles M. Bowden, Jonathan P. Dowling, and Henry O. Everitt; it took place in February at the University of Arizona in Tucson.
- Peter Shor proposes the first schemes for quantum error correction.[25]
- Christopher Monroe and David Wineland at NIST (Boulder, Colorado) experimentally realize the first quantum logic gate – the controlled-NOT gate – with trapped ions, following the Cirac-Zoller proposal.[26]
- independently, Subhash Kak and Ronald Chrisley propose the first quantum neural network[27][28]

1996

- Lov Grover, at Bell Labs, invents the quantum database search algorithm. The quadratic speedup is not as dramatic as the speedup for factoring, discrete logs, or physics simulations. However, the algorithm can be applied to a much wider variety of problems. Any problem that can be solved by random, brute-force search, may take advantage of this quadratic speedup in the number of search queries.
- The United States Government, particularly in a joint partnership of the Army Research Office (now part of the Army Research Laboratory) and the National Security Agency, issues the first public call for research proposals in quantum information processing.
- Andrew Steane designs Steane codes for error correction.[29]
- David P. DiVincenzo, of IBM, proposes a list of minimal requirements for creating a quantum computer,[30] now called DiVincenzo's criteria.

1997

- David Cory, Amr Fahmy and Timothy Havel, and at the same time Neil Gershenfeld and Isaac L. Chuang at MIT publish the first papers realizing gates for quantum computers

based on bulk nuclear spin resonance, or thermal ensembles. The technology is based on a nuclear magnetic resonance (NMR) machine, which is similar to the medical magnetic resonance imaging machine.
- Alexei Kitaev describes the principles of topological quantum computation as a method for dealing with the problem of decoherence.[31]
- Daniel Loss and David P. DiVincenzo propose the Loss-DiVincenzo quantum computer, using as qubits the intrinsic spin-1/2 degree of freedom of individual electrons confined to quantum dots.[32]

1998

- The first experimental demonstration of a quantum algorithm is reported. A working 2-qubit NMR quantum computer was used to solve Deutsch's problem by Jonathan A. Jones and Michele Mosca at Oxford University and shortly after by Isaac L. Chuang at IBM's Almaden Research Center, in California, and Mark Kubinec and the University of California, Berkeley together with coworkers at Stanford University and MIT.[33]
- The first working 3-qubit NMR computer is reported.
- Bruce Kane proposes a silicon-based nuclear spin quantum computer, using nuclear spins of individual phosphorus atoms in silicon as the qubits and donor electrons to mediate the coupling between qubits.[34]
- The first execution of Grover's algorithm on an NMR computer is reported.[35]
- Hidetoshi Nishimori & colleagues from Tokyo Institute of Technology show that a quantum annealing algorithm can perform better than classical simulated annealing under certain conditions.[36]
- Daniel Gottesman and Emanuel Knill independently prove that a certain subclass of quantum computations can be efficiently emulated with classical resources (Gottesman–Knill theorem).[37]

1999

- Samuel L. Braunstein and collaborators show that none of the bulk NMR experiments performed to date contain any entanglement; the quantum states being too strongly mixed. This is seen as evidence that NMR computers would likely not yield a benefit over classical computers. It remains an open question, however, whether entanglement is necessary for quantum computational speedup.[38]
- Gabriel Aeppli, Thomas Felix Rosenbaum and colleagues demonstrate experimentally the basic concepts of quantum annealing in a condensed matter system.
- Yasunobu Nakamura and Jaw-Shen Tsai demonstrate that a superconducting circuit can be used as a qubit.[39]

2000s

2000

- Arun K. Pati and Samuel L. Braunstein prove the quantum no-deleting theorem. This is dual to the no-cloning theorem which shows that one cannot delete a copy of an unknown qubit. Together with the stronger no-cloning theorem, the no-deleting theorem has the implication that quantum information can neither be created nor be destroyed.

- The first working 5-qubit NMR computer is demonstrated at the Technical University of Munich, Germany.
- The first execution of order finding (part of Shor's algorithm) at IBM's Almaden Research Center and Stanford University is demonstrated.
- The first working 7-qubit NMR computer is demonstrated at the Los Alamos National Laboratory in New Mexico.
- The textbook, *Quantum Computation and Quantum Information*, by Michael Nielsen and Isaac Chuang is published.

2001

- The first execution of Shor's algorithm at IBM's Almaden Research Center and Stanford University is demonstrated. The number 15 was factored using 10^{18} identical molecules, each containing seven active nuclear spins.
- Noah Linden and Sandu Popescu prove that the presence of entanglement is a necessary condition for a large class of quantum protocols. This, coupled with Braunstein's result (see 1999 above), called the validity of NMR quantum computation into question.[40]
- Emanuel Knill, Raymond Laflamme, and Gerard Milburn show that optical quantum computing is possible with single-photon sources, linear optical elements, and single-photon detectors, establishing the field of linear optical quantum computing.
- Robert Raussendorf and Hans Jürgen Briegel propose measurement-based quantum computation.[41]

2002

- The Quantum Information Science and Technology Roadmapping Project, involving some of the main participants in the field, lays out the Quantum computation roadmap.
- The Institute for Quantum Computing is established at the University of Waterloo in Waterloo, Ontario by Mike Lazaridis, Raymond Laflamme and Michele Mosca.[42]
- A group led by Gerhard Birkl (now at TU Darmstadt) demonstrates the first 2D array of optical tweezers with trapped atoms for quantum computation with atomic qubits.[43]

2003

- Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer at the University of Innsbruck is reported.[44]
- Todd D. Pittman and collaborators at Johns Hopkins University, Applied Physics Laboratory, and independently Jeremy L. O'Brien and collaborators at the University of Queensland, demonstrate quantum controlled-not gates using only linear optical elements.[45][46]
- The first implementation of a CNOT quantum gate, according to the Cirac–Zoller proposal, is reported by a team at the University of Innsbruck led by Rainer Blatt.[47]
- The DARPA Quantum Network becomes fully operational on October 23, 2003.

- The Institute for Quantum Optics and Quantum Information (IQOQI) is established in Innsbruck and Vienna, Austria, by the founding directors Rainer Blatt, Hans Jürgen Briegel, Rudolf Grimm, Anton Zeilinger and Peter Zoller.

2004

- The first working pure state NMR quantum computer (based on parahydrogen) is demonstrated at Oxford University, England and University of York, England.
- Physicists at the University of Innsbruck show deterministic quantum-state teleportation between a pair of trapped calcium ions.[48]
- The first five-photon entanglement is demonstrated by Jian-Wei Pan's team at the University of Science and Technology of Chin; the minimal number of qubits required for universal quantum error correction.[49]

2005

- University of Illinois at Urbana–Champaign scientists demonstrate quantum entanglement of multiple characteristics, potentially allowing multiple qubits per particle.
- Two teams of physicists measure the capacitance of a Josephson junction for the first time. The methods could be used to measure the state of quantum bits in a quantum computer without disturbing the state.[50]
- In December, W-states of quantum registers with up to 8 qubits implemented using trapped ions are demonstrated at the Institute for Quantum Optics and Quantum Information and the University of Innsbruck in Austria.[51]
- Harvard University and Georgia Institute of Technology researchers succeed in transferring quantum information between "quantum memories" – from atoms to photons and back again.

2006

- The Materials Science Department of Oxford University, England cage a qubit in a "buckyball" (a molecule of buckminsterfullerene) and demonstrated quantum "bang-bang" error correction.[52]
- Researchers from the University of Illinois at Urbana–Champaign use the Zeno Effect, repeatedly measuring the properties of a photon to gradually change it without actually allowing the photon to reach the program, to search a database using counterfactual quantum computation.[53]
- Vlatko Vedral of the University of Leeds and colleagues at the universities of Porto and Vienna find that the photons in ordinary laser light can be quantum mechanically entangled with the vibrations of a macroscopic mirror.[54]
- Samuel L. Braunstein at the University of York along with the University of Tokyo and the Japan Science and Technology Agency give the first experimental demonstration of quantum telecloning.[55]
- Professors at the University of Sheffield develop a means to efficiently produce and manipulate individual photons at high efficiency at room temperature.[56]
- A new error checking method is theorized for Josephson junction computers.[57]
- The first 12-qubit quantum computer is benchmarked by researchers at the Institute for Quantum Computing and the Perimeter Institute for Theoretical Physics in Waterloo, Ontario

as well as at MIT, Cambridge.[58]

- A two-dimensional ion trap is developed for quantum computing.[59]
- Seven atoms are placed in a stable line, a step on the way to constructing a quantum gate, at the University of Bonn.[60]
- A team at Delft University of Technology in the Netherlands creates a device that can manipulate the "up" or "down" spin-states of electrons on quantum dots.[61]
- The University of Arkansas develops quantum dot molecules.[62]
- The spinning new theory on particle spin brings science closer to quantum computing.[63]
- The University of Copenhagen develops quantum teleportation between photons and atoms.[64]
- University of Camerino scientists develop a theory of macroscopic object entanglement, which has implications for the development of quantum repeaters.[65]
- Tai-Chang Chiang, at Illinois at Urbana–Champaign, finds that quantum coherence can be maintained in mixed-material systems.[66]
- Cristophe Boehme, University of Utah, demonstrates the feasibility of reading data using the nuclear spin on a silicon-phosphorus Kane quantum computer.[67]

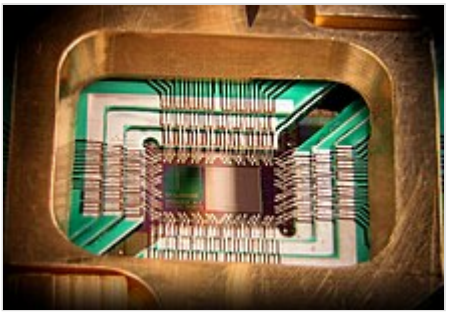
2007

- Subwavelength waveguide is developed for light.[68]
- A single-photon emitter for optical fibers is developed.[69]
- The first one-way quantum computers are built,[70] where measurement (collapse) of an entangled cluster state is the main driving force of computation,[71] and shown to perform simple computations, such as Deutsch's algorithm.[72]
- A new material is proposed for quantum computing.[73]
- A single-atom single-photon server is devised.[74]
- The University of Cambridge develops an electron quantum pump.[75]
- A superior method of qubit coupling is developed.[76]
- A successful demonstration of controllably coupled qubits is reported.[77]
- A breakthrough in applying spin-based electronics to silicon is reported.[78]
- Scientists demonstrate a quantum state exchange between light and matter.[79]
- A diamond quantum register is developed.[80]
- Controlled-NOT quantum gates on a pair of superconducting quantum bits are realized.[81]
- Scientists contain and study hundreds of individual atoms in 3D array.[82]
- Nitrogen in a buckyball molecule is used in quantum computing.[83]
- A large number of electrons are quantum coupled.[84]
- Spin–orbit interaction of electrons are measured.[85]
- Atoms are quantum manipulated in laser light.[86]
- Light pulses are used to control electron spins.[87]
- Quantum effects are demonstrated across tens of nanometers.[88]
- Light pulses are used to accelerate quantum computing development.[89]
- A quantum RAM blueprint is unveiled.[90]
- A model of a quantum transistor is developed.[91]

- Long distance entanglement is demonstrated.[92]
- Photonic quantum computing is used to factor a number by two independent labs.[93]
- A quantum bus is developed by two independent labs.[94]
- A superconducting quantum cable is developed.[95]
- The transmission of qubits is demonstrated.[96]
- Superior qubit material is devised.[97]
- A single-electron qubit memory is reported.[98]
- Bose–Einstein condensate quantum memory is developed.[99]
- D-Wave Systems demonstrates use of a 28-qubit quantum annealing computer.[100]
- A new cryonic method reduces decoherence and increases interaction distance, and thus quantum computing speed.[101]
- A photonic quantum computer is demonstrated.[102]
- Graphene quantum dot spin qubits are proposed.[103]

2008

- The HHL algorithm for solving linear equations is published.[104]
- Graphene quantum dot qubits are described.[105]
- Scientists succeed in storing a quantum bit.[106]
- 3D qubit-qutrit entanglement is demonstrated.[107]
- Analog quantum computing is devised.[108]
- Control of quantum tunneling is devised.[109]
- Entangled memory is developed.[110]
- A superior NOT gate is developed.[111]
- Qutrits are developed.[112]
- Quantum logic gate in optical fiber[113]
- A superior quantum Hall Effect is discovered.[114]
- Enduring spin states in quantum dots are reported.[115]
- Molecular magnets are proposed for quantum RAM.[116]
- Quasiparticles offer hope of stable quantum computers.[117]
- Image storage may have better storage of qubits is reported.[118]
- Quantum entangled images are reported.[119]
- Quantum state is intentionally altered in a molecule.[120]
- Electron position is controlled in a silicon circuit.[121]
- A superconducting electronic circuit pumps microwave photons.[122]
- Amplitude spectroscopy is developed.[123]
- A superior quantum computer test is developed.[124]
- An optical frequency comb is devised.[125]
- The concept of Quantum Darwinism is supported.[126]
- Hybrid qubit memory is developed.[127]
- A qubit is stored for over 1 second in an atomic nucleus.[128]



Chip constructed by D-Wave Systems Inc. designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor, mounted in a sample holder (2009)

- Faster electron spin qubit switching and reading is developed.[129]
- The possibility of non-entanglement quantum computing is described.[130]
- D-Wave Systems claim to have produced a 128 qubit computer chip, though this claim had yet to be verified.[131]

2009

- Carbon 12 is purified for longer coherence times.[132]
- The lifetime of qubits is extended to hundreds of milliseconds.[133]
- Improved quantum control of photons is reported.[134]
- Quantum entanglement is demonstrated over 240 micrometres.[135]
- Qubit lifetime is extended by a factor of 1000.[136]
- The first electronic quantum processor is created.[137]
- Six-photon graph state entanglement is used to simulate the fractional statistics of anyons living in artificial spin-lattice models.[138]
- A single-molecule optical transistor is devised.[139]
- NIST is reads and writes individual qubits.[140]
- NIST demonstrates multiple computing operations on qubits.[141]
- The first large-scale topological cluster state quantum architecture is developed for atom-optics.[142]
- A combination of all of the fundamental elements required to perform scalable quantum computing through the use of qubits stored in the internal states of trapped atomic ions is shown.[143]
- Researchers at University of Bristol demonstrate Shor's algorithm on a silicon photonic chip.[144]
- Quantum Computing with an Electron Spin Ensemble is reported.[145]
- A so-called photon machine gun is developed for quantum computing.[146]
- The first universal programmable quantum computer is unveiled.[147]
- Scientists electrically control quantum states of electrons.[148]
- Google collaborates with D-Wave Systems on image search technology using quantum computing.[149]
- A method for synchronizing the properties of multiple coupled CJJ rf-SQUID flux qubits with a small spread of device parameters due to fabrication variations is demonstrated.[150]
- Universal Ion Trap Quantum Computation with decoherence free qubits is realized.[151]
- The first chip-scale quantum computer is reported.[152]

2010s

2010

- Ions were trapped in an optical trap.[153]
- An optical quantum computer with three qubits calculated the energy spectrum of molecular hydrogen to high precision.[154]

- The first germanium laser advanced the state of optical computers.[155]
- A single-electron qubit was developed[156]
- The quantum state in a macroscopic object was reported.[157]
- A new quantum computer cooling method was developed.[158]
- Racetrack ion trap was developed.[159]
- Evidence for a Moore-Read state in the $u = 5/2$ quantum Hall plateau,[160] which would be suitable for topological quantum computation was reported
- A quantum interface between a single photon and a single atom was demonstrated.[161]
- LED quantum entanglement was demonstrated.[162]
- Multiplexed design increased the speed of transmission of quantum information through a quantum communications channel.[163]
- A two-photon optical chip was reported.[164]
- Microfabricated planar ion traps were tested.[165][166]
- A boson sampling technique was proposed by Aaronson and Arkhipov.[167]
- Quantum dot qubits were manipulated electrically, not magnetically.[168]

2011

- Entanglement in a solid-state spin ensemble was reported[169]
- NOON photons in a superconducting quantum integrated circuit were reported.[170]
- A quantum antenna was described.[171]
- Multimode quantum interference was documented.[172]
- Magnetic Resonance applied to quantum computing was reported.[173]
- The quantum pen for single atoms was documented.[174]
- Atomic "Racing Dual" was reported.[175]
- A 14 qubit register was reported.[176]
- D-Wave claimed to have developed quantum annealing and introduced their product called D-Wave One. The company claims this is the first commercially available quantum computer.[177]
- Repetitive error correction was demonstrated in a quantum processor.[178]
- Diamond quantum computer memory was demonstrated.[179]
- Qmodes were developed.[180]
- Decoherence was demonstrated as suppressed.[181]
- Simplification of controlled operations was reported.[182]
- Ions entangled using microwaves were documented.[183]
- Practical error rates were achieved.[184]
- A quantum computer employing Von Neumann architecture was described.[185]
- A quantum spin Hall topological insulator was reported.[186]

- The concept of two diamonds linked by quantum entanglement could help develop photonic processors was described.[187]

2012

- D-Wave claimed a quantum computation using 84 qubits.[188]
- Physicists created a working transistor from a single atom.[189][190]
- A method for manipulating the charge of nitrogen vacancy-centres in diamond was reported.[191]
- Creation of a 300 qubit/particle quantum simulator was reported.[192][193]
- Demonstration of topologically protected qubits with an eight-photon entanglement was reported; a robust approach to practical quantum computing.[194]
- 1QB Information Technologies (1QBit) was founded; the world's first dedicated quantum computing software company.[195]
- The first design of a quantum repeater system without a need for quantum memories was reported.[196]
- Decoherence suppressed for 2 seconds at room temperature by manipulating Carbon-13 atoms with lasers was reported.[197][198]
- The theory of Bell-based randomness expansion with reduced assumption of measurement independence was reported.[199]
- New low overhead method for fault-tolerant quantum logic was developed called lattice surgery.[200]

2013

- Coherence time of 39 minutes at room temperature (and 3 hours at cryogenic temperatures) was demonstrated for an ensemble of impurity-spin qubits in isotopically purified silicon.[201]
- Extension of time for a qubit maintained in superimposed state for ten times longer than what has ever been achieved before was reported.[202]
- The first resource analysis of a large-scale quantum algorithm using explicit fault-tolerant, error-correction protocols was developed for factoring.[203]

2014

- Documents leaked by Edward Snowden confirmed the Penetrating Hard Targets project,[204] by which the National Security Agency sought to develop a quantum computing capability for cryptography purposes.[205][206][207]
- Researchers in Japan and Austria published the first large-scale quantum computing architecture for a diamond-based system.[208]
- Scientists at the University of Innsbruck performed quantum computations on a topologically encoded qubit which was encoded in entangled states distributed over seven trapped-ion qubits.[209]

- Scientists transferred data by quantum teleportation over a distance of 10 feet (3.0 meters) with zero percent error rate; a vital step towards a quantum Internet.[210][211]

2015

- Optically addressable nuclear spins in a solid with a six-hour coherence time were documented.[212]
- Quantum information encoded by simple electrical pulses was documented.[213]
- Quantum error detection code using a square lattice of four superconducting qubits was documented.[214]
- D-Wave Systems Inc. announced on June 22 that it had broken the 1,000-qubit barrier.[215]
- A two-qubit silicon logic gate was successfully developed.[216]

2016

- Physicists led by Rainer Blatt joined forces with scientists at the Massachusetts Institute of Technology (MIT), led by Isaac Chuang, to efficiently implement Shor's algorithm in an ion-trap-based quantum computer.[217]
- IBM released the Quantum Experience, an online interface to their superconducting systems. The system is immediately used to publish new protocols in quantum information processing.[218][219]
- Google, using an array of 9 superconducting qubits developed by the Martinis group and UCSB, simulated a hydrogen molecule.[220]
- Scientists in Japan and Australia invented a quantum version of a Sneakernet communications system.[221]

2017

- D-Wave Systems Inc. announced general commercial availability of the D-Wave 2000Q quantum annealer, which it claimed has 2000 qubits.[222]
- A blueprint for a microwave trapped ion quantum computer was published.[223]
- IBM unveiled a 17-qubit quantum computer—and a better way of benchmarking it.[224]
- Scientists built a microchip that generates two entangled qudits each with 10 states, for 100 dimensions total.[225]
- Microsoft revealed Q#, a quantum programming language integrated with its Visual Studio development environment. Programs can be executed locally on a 32-qubit simulator, or a 40-qubit simulator on Azure.[226]
- IBM revealed a working 50-qubit quantum computer that can maintain its quantum state for 90 microseconds.[227]
- The first teleportation using a satellite, connecting ground stations over a distance of 1400 km apart was announced.[228] Previous experiments were at Earth, at shorter distances.

2018

- John Preskill introduces the concept of noisy intermediate-scale quantum (NISQ) era.[229]

- MIT scientists reported the discovery of a new triple-photon form of light.[230][231]
- Oxford researchers successfully use a trapped-ion technique, where they placed two charged atoms in a state of quantum entanglement to speed up logic gates by a factor of 20 to 60 times, as compared with the previous best gates, translated to 1.6 microseconds long, with 99.8% precision.[232]
- QuTech successfully tested a silicon-based 2-spin-qubit processor.[233]
- Google announced the creation of a 72-qubit quantum chip, called "Bristlecone",[234] achieving a new record.
- Intel began testing a silicon-based spin-qubit processor manufactured in the company's D1D fab in Oregon.[235]
- Intel confirmed development of a 49-qubit superconducting test chip, called "Tangle Lake".[236]
- Japanese researchers demonstrated universal holonomic quantum gates.[237]
- An integrated photonic platform for quantum information with continuous variables was documented.[238]
- On December 17, 2018, the company IonQ introduced the first commercial trapped-ion quantum computer, with a program length of over 60 two-qubit gates, 11 fully connected qubits, 55 addressable pairs, one-qubit gate error of <0.03% and two-qubit gate error of <1.0%.[239][240]
- On December 21, 2018, the National Quantum Initiative Act was signed into law by President Donald Trump, establishing the goals and priorities for a 10-year plan to accelerate the development of quantum information science and technology applications in the United States.[241][242][243]

2019



IBM Q System One (2019), the first circuit-based commercial quantum computer

- IBM unveiled its first commercial quantum computer, the IBM Q System One,[244] designed by UK-based Map Project Office and Universal Design Studio and manufactured by Goppion.[245]
- Austrian physicists demonstrated self-verifying, hybrid, variational quantum simulation of lattice models in condensed matter and high-energy physics using a feedback loop between a classical computer and a quantum co-processor.[246]
- Griffith University, UNSW and UTS, in partnership with seven universities in the United States, develop noise cancelling for quantum bits via machine learning, taking quantum noise in a quantum chip down to 0%.[247][248]
- Quantum Darwinism was observed in diamond at room temperature.[249][250]
- Google revealed its Sycamore processor, consisting of 53 qubits. A paper by Google's quantum computer research team was briefly available in late September 2019, claiming the project had reached quantum supremacy.[251][252][253] Google also developed a cryogenic chip for controlling qubits from within a dilution refrigerator.[254]

- University of Science and Technology of China researchers demonstrated boson sampling with 14 detected photons.[255]

2020s

2020

- 20 April – UNSW Sydney develops a way of producing 'hot qubits' – quantum devices that operate at 1.5 kelvin.[256]
- 11 March – UNSW perform electric nuclear resonance to control single atoms in electronic devices.[257]
- 23 April – University of Tokyo and Australian scientists create and successfully test a solution to the quantum wiring problem, creating a 2D structure for qubits. Such structure can be built using existing integrated circuit technology and has considerably lower cross-talk.[258]
- 16 January – Quantum physicists report the first direct splitting of one photon into three using spontaneous parametric down-conversion which may have applications in quantum technology.[259][260]
- 11 February – Quantum engineers report that they created artificial atoms in silicon quantum dots for quantum computing and that artificial atoms with a higher number of electrons can be more stable qubits than previously thought possible. Enabling silicon-based quantum computers may make it possible to reuse the manufacturing technology of "classical" modern-day computer chips among other advantages.[261][262]
- 14 February – Quantum physicists develop a novel single-photon source which may allow bridging of semiconductor-based quantum-computers that use photons by converting the state of an electron spin to the polarisation of a photon. They showed that they can generate a single photon in a controlled way without the need for randomly formed quantum dots or structural defects in diamonds.[263][264]
- 25 February – Scientists visualize a quantum measurement: by taking snapshots of ion states at different times of measurement via coupling of a trapped ion qutrit to the photon environment, they showed that the changes of the degrees of superpositions, and therefore of probabilities of states after measurement, happens gradually under the measurement influence.[265][266]
- 2 March – Scientists report achieving repeated quantum nondemolition measurements of an electron's spin in a silicon quantum dot: measurements that do not change the electron's spin in the process.[267][268]
- 11 March – Quantum engineers report to have controlled the nucleus of a single atom using only electric fields. This was first suggested to be possible in 1961 and may be used for silicon quantum computers that use single-atom spins without needing oscillating magnetic fields. This may be especially useful for nanodevices, for precise sensors of electric and magnetic fields, as well as for fundamental inquiries into quantum nature.[269][270]
- 19 March – A US Army laboratory announces that its scientists analysed a Rydberg sensor's sensitivity to oscillating electric fields over an enormous range of frequencies—from 0 to 10^12 Hz (the spectrum to 0.3 mm wavelength). The Rydberg sensor may potentially be used to detect communications signals as it could reliably detect signals over the entire spectrum and compare favourably with other established electric field sensor technologies, such as electro-optic crystals and dipole antenna-coupled passive electronics.[271][272]
- 23 March – Researchers report that they corrected for signal loss in a prototype quantum node that can catch, store and entangle bits of quantum information. Their concepts could

be used for key components of quantum repeaters in quantum networks and extend their longest possible range.[273][274]

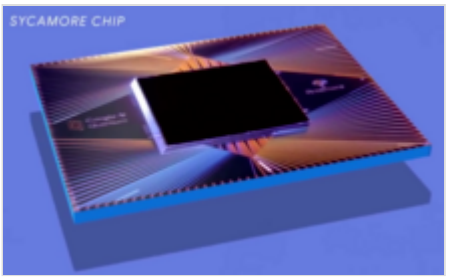
- 15 April – Researchers demonstrate a proof-of-concept silicon quantum processor unit cell which works at 1.5 kelvin – many times warmer than common quantum processors that are being developed. The finding may enable the integration of classical control electronics with a qubit array and substantially reduce costs. The cooling requirements necessary for quantum computing have been called one of the toughest roadblocks in the field.[275][276][277][278]
- 16 April – Scientists prove the existence of the Rashba effect in bulk perovskites. Previously researchers have hypothesized that the materials' extraordinary electronic, magnetic and optical properties – which make it a commonly used material for solar cells and quantum electronics – are related to this effect which to date had not been proven to be present in the material.[279][280]



Working IQM Quantum Computer installed in Espoo, Finland in 2020

- 8 May – Researchers report to have developed a proof-of-concept of a quantum radar using quantum entanglement and microwaves which may potentially be useful for the development of improved radar systems, security scanners and medical imaging systems.[281][282][283]
- 12 May – Researchers report to have developed a method to selectively manipulate a layered manganite's correlated electrons' spin state while leaving its orbital state intact using femtosecond X-ray laser pulses. This may indicate that orbitronics – using variations in the orientations of orbitals – may be used as the basic unit of information in novel IT devices.[284][285]
- 19 May – Researchers report to have developed the first integrated silicon on-chip low-noise single-photon source compatible with large-scale quantum photonics.[286][287][288]
- 11 June – Scientists report the generation of rubidium Bose–Einstein condensates (BECs) in the Cold Atom Laboratory aboard the International Space Station under microgravity which could enable improved research of BECs and quantum mechanics, whose physics are scaled to macroscopic scales in BECs, support long-term investigations of few-body physics, support the development of techniques for atom–wave interferometry and atom lasers and verified the successful operation of the laboratory.[289][290][291]
- 15 June – Scientists report the development of the smallest synthetic molecular motor, consisting of 12 atoms and a rotor of 4 atoms, shown to be capable of being powered by an electric current using an electron scanning microscope and moving even with very low amounts of energy due to quantum tunneling.[292][293][294]
- 17 June – Quantum scientists report the development of a system that entangled two photon quantum communication nodes through a microwave cable that can send information in between without the photons being sent through, or occupying, the cable. On 12 June it was reported that they also, for the first time, entangled two phonons as well as erase information from their measurement after the measurement had been completed using delayed-choice quantum erasure.[295][296][297][298]
- 18 June – Honeywell announces a quantum computer with a quantum volume of 64, the highest at the time.[299]
- 13 August – Universal coherence protection is reported to have been achieved in a solid-state spin qubit, a modification that allows quantum systems to stay operational (or "coherent") for 10,000 times longer than before.[300][301]

- 26 August – Scientists report that ionizing radiation from environmental radioactive materials and cosmic rays may substantially limit the coherence times of qubits if they are not shielded adequately.[302][303][304]
- 28 August – Quantum engineers working for Google report the largest chemical simulation on a quantum computer – a Hartree–Fock approximation with a Sycamore computer paired with a classical computer that analyzed results to provide new parameters for a 12-qubit system.[305][306][307]
- 2 September – Researchers present an eight-user city-scale quantum communication network, located in Bristol, England, using already deployed fibres without active switching or trusted nodes.[308][309]
- 9 September – Xanadu offers a cloud quantum computing service, offering a photonic quantum computer.[310]



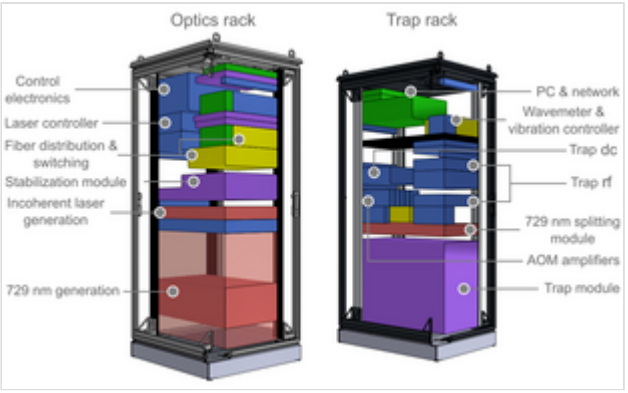
Google Sycamore quantum computer processor in 2019

- 21 September – Researchers report the achievement of quantum entanglement between the motion of a millimetre-sized mechanical oscillator and a disparate distant spin system of a cloud of atoms.[311][312]
- 3 December – Chinese researchers claim to have achieved quantum supremacy, using a photonic peak 76-qubit system (43 average) known as *Jiuzhang*, which performed calculations at 100 trillion times the speed of classical supercomputers.[313][314][315]
- 29 October – Honeywell introduces a subscription for a quantum computing service, known as quantum computing as a service,, with an ion trap quantum computer.[316]
- 12 December – At the IEEE International Electron Devices Meeting (IEDM), IMEC shows an RF multiplexer chip that operates at temperatures as low as a few milikelvins, designed for quantum computers. Researchers from the Chalmers University of Technology developed a cryogenic low-noise amplifier (LNA) for amplifying signals from qubits, made of indium phosphide (InP) high-electron-mobility transistors (HEMTs).[317]
- 21 December – Publication of research of "counterfactual quantum communication" – whose first achievement was reported in 2017 – by which information can be exchanged without any physical particle traveling between observers and without quantum teleportation.[318] The research suggests that this is based on some form of relation between the properties of modular angular momentum.[319][320][321]

2021

- 6 January – Chinese researchers report that they have built the world's largest integrated quantum communication network, combining over 700 optical fibers with two QKD-ground-to-satellite links for a total distance between nodes of the network of networks of up to ~4,600 km.[322][323]
- 13 January – Austrian researchers report the first realization of an entangling gate between two logical qubits encoded in topological quantum error-correction codes using a trapped-ion quantum computer with 10 ions.[324][325]
- 15 January – Researchers in China report the successful transmission of entangled photons between drones, used as nodes for the development of mobile quantum networks or flexible network extensions, marking the first work in which entangled particles were sent between two moving devices.[326][327]
- 27 January – BMW announces the use of a quantum computer for the optimization of supply chains.[328]

- 28 January – Swiss and German researchers report the development of a highly efficient single-photon source for quantum IT with a system of gated quantum dots in a tunable microcavity which captures photons released from these excited "artificial atoms".[329][330]
- 3 February – Microsoft starts offering a cloud quantum computing service, called Azure Quantum.[331]
- 5 February – Researchers demonstrate a first prototype of quantum-logic gates for distributed quantum computers.[332][333]
- 11 March – Honeywell announces a quantum computer with a quantum volume of 512.[334]
- 13 April – In a preprint, an astronomer describes for the first time how one could search for quantum communication transmissions sent by extraterrestrial intelligence using existing telescope and receiver technology. He also provides arguments for why future searches of SETI should also target interstellar quantum communications.[335][336]
- 7 May – Two studies complement research published September 2020 by quantum-entangling two mechanical oscillators.[337][338][339]
- 8 June – Researchers from Toshiba achieve quantum communications over optical fibres exceeding 600 km in length, a world-record distance.[340][341][342]
- 17 June – Austrian, German and Swiss researchers present a quantum computing demonstrator fitting into two 19-inch racks, the world's first quality standards-meeting compact quantum computer.[343][344]



- 29 June – IBM demonstrates a quantum advantage.[345]
- 1 July – Rigetti develops a method to join several quantum processor chips together.[346]
- 7 July – American researchers present a programmable quantum simulator that can operate with 256 qubits,[347][348] and on the same date and journal another team presents a quantum simulator of 196 Rydeberg atoms trapped in optical tweezers.[349]
- 25 October – Chinese researchers report that they have developed the world's fastest programmable quantum computers. The photon-based *Jiuzhang 2* is claimed to calculate a task in one millisecond, that otherwise would have taken a conventional computer 30 trillion years to complete. Additionally, *Zuchongzhi 2* is a 66-qubit programmable superconducting quantum computer that was claimed to be the world's fastest quantum computer that can run a calculation task one million times more complex than Google's Sycamore, as well as being 10 million times faster.[350][351]
- 11 November – The first simulation of baryons on a quantum computer is reported by University of Waterloo.[352][353]
- 16 November – IBM claims that it has created a 127 quantum bit processor, 'IBM Eagle', which according to a report is the most powerful quantum processor known. According to the report, the company had not yet published an academic paper describing its metrics, performance or abilities.[354][355]

2022

- 18 January – Europe's first quantum annealer with more than 5,000 qubits is presented in Jülich, Germany.[356]

- 24 March – The first prototype, photonic, quantum memristive device, for neuromorphic (quantum-) computers and artificial neural networks, that is "able to produce memristive dynamics on single-photon states through a scheme of measurement and classical feedback" is invented.[357][358]
- 14 April – The Quantinuum System Model H1-2 doubles its performance claiming to be the first commercial quantum computer to pass quantum volume 4096.[359]
- 26 May – A universal set of computational operations on fault-tolerant quantum bits is demonstrated by a team of experimental physicists in Innsbruck, Austria.[360]
- 22 June – The world's first quantum computer integrated circuit is demonstrated.[361][362]
- 28 June – Physicists report that interstellar quantum communication by other civilizations could be possible and may be advantageous, identifying some potential challenges and factors for detecting such. They may use, for example, X-ray photons for remotely established quantum communications and quantum teleportation as the communication mode.[363][364]
- 21 July – A universal qudit quantum processor is demonstrated with trapped ions.[365]
- 15 August – *Nature Materials* publishes the first work showing optical initialization and coherent control of nuclear spin qubits in 2D materials (an ultrathin hexagonal boron nitride).[366]
- 24 August – *Nature* publishes the first research related to a set of 14 photons entangled with high efficiency and in a defined way.[367]
- 26 August – Created photon pairs at several different frequencies using optical ultra-thin resonant metasurfaces made up of arrays of nanoresonators is reported.[368]
- 29 August – Physicists at the Max Planck Institute for Quantum Optics deterministically generate entangled graph states of up to 14 photons using a trapped rubidium atom in an optical cavity.[369]
- 2 September – Researchers from The University of Tokyo and other Japanese institutions develop a systematic method that applies optimal control theory (GRAPE algorithm) to identify the theoretically optimal sequence from among all conceivable quantum operation sequences. It is necessary to complete the operations within the time that the coherent quantum state is maintained.[370]
- 30 September – Researchers at University of New South Wales achieve a coherence time of two milliseconds, 100 times higher than the previous benchmark in the same quantum processor.[371]
- 9 November – IBM presents its 433-qubit 'Osprey' quantum processor, the successor to its Eagle system.[372][373]
- 1 December – The world's first portable quantum computer enters into commerce in Japan. With three variants, topping out at 3 qubits, they are meant for education. They are based on nuclear magnetic resonance (NMR), "NMR has extremely limited scaling capabilities" and dimethylphosphite.[374][375][376]

2023

- 3 February – At the University of Innsbruck, researchers entangle two ions over a distance of 230 meters.[377]
- 8 February – Alpine Quantum Technologies (AQT) demonstrates a quantum volume of 128 on its 19-inch rack-compatible quantum computer system PINE – a new record in Europe.[378]
- 17 February - Fusion-based quantum computation is proposed[379]

- 27 March – India's first quantum computing-based telecom network link is inaugurated.[380]
- 14 June – IBM computer scientists report that a quantum computer produced better results for a physics problem than a conventional supercomputer.[381][382]
- 21 June – Microsoft declares that it is working on a topological quantum computer based on Majorana fermions, with the aim of arriving within 10 years at a computer capable of carrying out at least one million operations per second with an error rate of one operation every 1,000 billion (corresponding to 11 uninterrupted days of calculation).[383]
- 13 October – Researchers at TU Darmstadt publish the first experimental demonstration of a qubit array with more than 1,000 qubits:[384][385] A 3,000-site atomic array based on a 2D configuration of optical tweezers[386] holds up to 1,305 atomic qubits.
- 24 October – Atom Computing announces that it has "created a 1,225-site atomic array, currently populated with 1,180 qubits",[387] based on Rydberg atoms.[388]
- 4 December – IBM presents its 1121-qubit 'Condor' quantum processor, the successor to its Osprey and Eagle systems.[389][390] The Condor system was the culmination of IBM's multi-year 'Roadmap to Quantum Advantage' seeking to break the 1,000 qubit threshold.[391]
- 6 December – A group led by Misha Lukin at Harvard University realises a programmable quantum processor based on logical qubits using reconfigurable neutral atom arrays.[392]

2024

- 8 May - Researchers deterministically fused small quantum states into states with up to eight qubits[393]
- 30 May - Researchers at Photonic and Microsoft performed a teleported CNOT gate between qubits physically separated by 40 meters, confirming remote quantum entanglement between T-centers.[394]

See also

- List of companies involved in quantum computing or communication
- List of quantum processors
- Category: Quantum information scientists
- Timeline of computing 2020–present

References

1. Mor, Tal; Renner, Renato (2014). "Preface". *Natural Computing*. **13** (4): 447–452. doi:10.1007/s11047-014-9464-3 (https://doi.org/10.1007%2Fs11047-014-9464-3).
2. Park, James (1970). "The concept of transition in quantum mechanics". *Foundations of Physics*. **1** (1): 23–33. Bibcode:1970FoPh....1...23P (https://ui.adsabs.harvard.edu/abs/1970FoPh....1...23P). CiteSeerX 10.1.1.623.5267 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.623.5267). doi:10.1007/BF00708652 (https://doi.org/10.1007%2FBF00708652). S2CID 55890485 (https://api.semanticscholar.org/CorpusID:55890485).
3. Bennett, C. (November 1973). "Logical Reversibility of Computation" (https://www.math.ucsd.edu/~sbuss/CourseWeb/Math268_2013W/Bennett_Reversibiity.pdf) (PDF). *IBM Journal of Research and Development*. **17** (6): 525–532. doi:10.1147/rd.176.0525 (https://doi.org/10.1147%2Frd.176.0525).

4. Poplavskii, R. P. (1975). "Thermodynamical models of information processing" (https://doi.org/10.3367%2FUFNr.0115.197503d.0465). *Uspekhi Fizicheskikh Nauk* (in Russian). **115** (3): 465–501. doi:10.3367/UFNr.0115.197503d.0465 (https://doi.org/10.3367%2FUFNr.0115.197503d.0465).
5. Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". *Journal of Statistical Physics*. **22** (5): 563–591. Bibcode:1980JSP....22..563B (https://ui.adsabs.harvard.edu/abs/1980JSP....22..563B). doi:10.1007/bf01011339 (https://doi.org/10.1007%2Fbf01011339). S2CID 122949592 (https://api.semanticscholar.org/CorpusID:122949592).
6. Manin, Yu I (1980). *Vychislimoe i nevychislimoe (Computable and Noncomputable)* (https://web.archive.org/web/20130510173823/http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.%281980%29.%5Bdjv%5D.zip) (in Russian). Soviet Radio. pp. 13–15. Archived from the original (http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) on May 10, 2013. Retrieved March 4, 2013.
7. Technical Report MIT/LCS/TM-151 (1980) and an adapted and condensed version: Toffoli, Tommaso (1980). "Reversible computing" (https://web.archive.org/web/20100415041123/http://pm1.bu.edu/~tt/publ/revcomp-rep.pdf) (PDF). In J. W. de Bakker and J. van Leeuwen (ed.). *Automata, Languages and Programming*. Automata, Languages and Programming, Seventh Colloquium. Lecture Notes in Computer Science. Vol. 85. Noordwijkerhout, Netherlands: Springer Verlag. pp. 632–644. doi:10.1007/3-540-10003-2_104 (https://doi.org/10.1007%2F3-540-10003-2_104). ISBN 3-540-10003-2. Archived from the original (http://pm1.bu.edu/~tt/publ/revcomp-rep.pdf) (PDF) on April 15, 2010.
8. Simson Garfinkel (April 27, 2021). "Tomorrow's computer, yesterday: Four decades ago at Endicott House, an MIT professor convened a conference that launched quantum computing" (https://www.technologyreview.com/2021/04/27/1021714/tomorrows-computer-yesterday/). *MIT News*. p. 10.
9. Benioff, Paul A. (April 1, 1982). "Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: Application to Turing machines". *International Journal of Theoretical Physics*. **21** (3): 177–201. Bibcode:1982IJTP...21..177B (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..177B). doi:10.1007/BF01857725 (https://doi.org/10.1007%2FBF01857725). ISSN 1572-9575 (https://search.worldcat.org/issn/1572-9575). S2CID 122151269 (https://api.semanticscholar.org/CorpusID:122151269).
10. "Simulating physics with computers" (https://web.archive.org/web/20190830190404/https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf) (PDF). Archived from the original (https://people.eecs.berkeley.edu/~christos/classics/Feynman.pdf) (PDF) on August 30, 2019. Retrieved July 5, 2023.
11. Benioff, Paul (1982). "Quantum mechanical hamiltonian models of turing machines". *Journal of Statistical Physics*. **29** (3): 515–546. Bibcode:1982JSP....29..515B (https://ui.adsabs.harvard.edu/abs/1982JSP....29..515B). doi:10.1007/BF01342185 (https://doi.org/10.1007%2FBF01342185). S2CID 14956017 (https://api.semanticscholar.org/CorpusID:14956017).
12. Wootters, William K.; Zurek, Wojciech H. (1982). "A single quantum cannot be cloned". *Nature*. **299** (5886): 802–803. Bibcode:1982Natur.299..802W (https://ui.adsabs.harvard.edu/abs/1982Natur.299..802W). doi:10.1038/299802a0 (https://doi.org/10.1038%2F299802a0). S2CID 4339227 (https://api.semanticscholar.org/CorpusID:4339227).
13. Dieks, Dennis (1982). "Communication by EPR devices". *Physics Letters A*. **92** (6): 271–272. Bibcode:1982PhLA...92..271D (https://ui.adsabs.harvard.edu/abs/1982PhLA...92..271D). CiteSeerX 10.1.1.654.7183 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.654.7183). doi:10.1016/0375-9601(82)90084-6 (https://doi.org/10.1016%2F0375-9601%2882%2990084-6).

14. Bennett, Charles H.; Brassard, Gilles (1984). "Quantum cryptography: Public key distribution and coin tossing" (https://doi.org/10.1016%2Fj.tcs.2014.05.025). *Theoretical Computer Science*. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. **560**: 7–11. arXiv:2003.06557 (https://arxiv.org/abs/2003.06557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025). ISSN 0304-3975 (https://search.worldcat.org/issn/0304-3975).
15. Peres, Asher (1985). "SReversible Logic and Quantum Compzters". *Physical Review A*. **32** (6): 3266–3276. Bibcode:1985PhRvA..32.3266P (https://ui.adsabs.harvard.edu/abs/1985PhRvA..32.3266P). doi:10.1103/PhysRevA.32.3266 (https://doi.org/10.1103%2FPhysRevA.32.3266). PMID 9896493 (https://pubmed.ncbi.nlm.nih.gov/9896493).
16. Igeta, K.; Yamamoto, Yoshihisa (July 18, 1988). "Quantum mechanical computers with single atom and photon fields" (https://opg.optica.org/abstract.cfm?uri=IQEC-1988-TuI4). *International Conference on Quantum Electronics (1988), Paper TuI4*. Optica Publishing Group: TuI4.
17. Milburn, Gerard J. (May 1, 1989). "Quantum optical Fredkin gate" (https://link.aps.org/doi/10.1103/PhysRevLett.62.2124). *Physical Review Letters*. **62** (18): 2124–2127. Bibcode:1989PhRvL..62.2124M (https://ui.adsabs.harvard.edu/abs/1989PhRvL..62.2124M). doi:10.1103/PhysRevLett.62.2124 (https://doi.org/10.1103%2FPhysRevLett.62.2124). PMID 10039862 (https://pubmed.ncbi.nlm.nih.gov/10039862).
18. Ray, P.; Chakrabarti, B. K.; Chakrabarti, A. (1989). "Sherrington-Kirkpatrick model in a transverse field: Absence of replica symmetry breaking due to quantum fluctuations". *Physical Review B*. **39** (16): 11828–11832. Bibcode:1989PhRvB..3911828R (https://ui.adsabs.harvard.edu/abs/1989PhRvB..3911828R). doi:10.1103/PhysRevB.39.11828 (https://doi.org/10.1103%2FPhysRevB.39.11828). PMID 9948016 (https://pubmed.ncbi.nlm.nih.gov/9948016).
19. Das, A.; Chakrabarti, B. K. (2008). "Quantum Annealing and Analog Quantum Computation". *Rev. Mod. Phys.* **80** (3): 1061–1081. arXiv:0801.2193 (https://arxiv.org/abs/0801.2193). Bibcode:2008RvMP...80.1061D (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1061D). CiteSeerX 10.1.1.563.9990 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.563.9990). doi:10.1103/RevModPhys.80.1061 (https://doi.org/10.1103%2FRevModPhys.80.1061). S2CID 14255125 (https://api.semanticscholar.org/CorpusID:14255125).
20. Ekert, A. K. (1991). "Quantum cryptography based on Bell's theorem". *Physical Review Letters*. **67** (6): 661–663. Bibcode:1991PhRvL..67..661E (https://ui.adsabs.harvard.edu/abs/1991PhRvL..67..661E). doi:10.1103/PhysRevLett.67.661 (https://doi.org/10.1103%2FPhysRevLett.67.661). PMID 10044956 (https://pubmed.ncbi.nlm.nih.gov/10044956). S2CID 27683254 (https://api.semanticscholar.org/CorpusID:27683254).
21. Waki, I.; Kassner, S.; Birkl, G.; Walther, H. (March 30, 1992). "Observation of ordered structures of laser-cooled ions in a quadrupole storage ring" (https://link.aps.org/doi/10.1103/PhysRevLett.68.2007). *Physical Review Letters*. **68** (13): 2007–2010. Bibcode:1992PhRvL..68.2007W (https://ui.adsabs.harvard.edu/abs/1992PhRvL..68.2007W). doi:10.1103/PhysRevLett.68.2007 (https://doi.org/10.1103%2FPhysRevLett.68.2007). PMID 10045280 (https://pubmed.ncbi.nlm.nih.gov/10045280).
22. Birkl, G.; Kassner, S.; Walther, H. (May 28, 1992). "Multiple-shell structures of laser-cooled 24Mg+ ions in a quadrupole storage ring" (https://doi.org/10.1038/357310a0). *Nature*. **357** (6376): 310–313. doi:10.1038/357310a0 (https://doi.org/10.1038%2F357310a0).
23. Raizen, M. G.; Gilligan, J. M.; Bergquist, J. C.; Itano, W. M.; Wineland, D. J. (May 1, 1992). "Ionic crystals in a linear Paul trap" (https://link.aps.org/doi/10.1103/PhysRevA.45.6493). *Physical Review A*. **45** (9): 6493–6501. Bibcode:1992PhRvA..45.6493R (https://ui.adsabs.harvard.edu/abs/1992PhRvA..45.6493R). doi:10.1103/PhysRevA.45.6493 (https://doi.org/10.1103%2FPhysRevA.45.6493). PMID 9907772 (https://pubmed.ncbi.nlm.nih.gov/9907772).

24. Chuang, Isaac L.; Yamamoto, Yoshihisa (1995). "Simple quantum computer". *Physical Review A*. **52** (5): 3489–3496. arXiv:quant-ph/9505011 (https://arxiv.org/abs/quant-ph/9505011). Bibcode:1995PhRvA..52.3489C (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.3489C). doi:10.1103/PhysRevA.52.3489 (https://doi.org/10.1103%2FPhysRevA.52.3489). PMID 9912648 (https://pubmed.ncbi.nlm.nih.gov/9912648).
25. Shor, Peter W. (1995). "Scheme for reducing decoherence in quantum computer memory". *Physical Review A*. **52** (4): R2493–R2496. Bibcode:1995PhRvA..52.2493S (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.2493S). doi:10.1103/PhysRevA.52.R2493 (https://doi.org/10.1103%2FPhysRevA.52.R2493). PMID 9912632 (https://pubmed.ncbi.nlm.nih.gov/9912632).
26. Monroe, C.; Meekhof, D. M.; King, B. E.; Itano, W. M.; Wineland, D. J. (December 18, 1995). "Demonstration of a Fundamental Quantum Logic Gate" (http://tf.nist.gov/general/pdf/140.pdf) (PDF). *Physical Review Letters*. **75** (25): 4714–4717. Bibcode:1995PhRvL..75.4714M (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75.4714M). doi:10.1103/PhysRevLett.75.4714 (https://doi.org/10.1103%2FPhysRevLett.75.4714). PMID 10059979 (https://pubmed.ncbi.nlm.nih.gov/10059979). Retrieved December 29, 2007.
27. Kak, S. C. (1995). "Quantum Neural Computing". *Advances in Imaging and Electron Physics*. **94**: 259–313. doi:10.1016/S1076-5670(08)70147-2 (https://doi.org/10.1016%2FS1076-5670%2808%2970147-2). ISBN 9780120147366.
28. Chrisley, R. (1995). Pyllkkänen, P.; Pyllkkö, P. (eds.). "Quantum learning" (https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a4051e9f560742b9d28afb78da4622141ec4db89). *New Directions in Cognitive Science*. Finnish Society for Artificial Intelligence.
29. Steane, Andrew (1996). "Multiple-Particle Interference and Quantum Error Correction" (https://web.archive.org/web/20060519062515/http://www.citebase.org/cgi-bin/citations?id=oai:arXiv.org:quant-ph/9601029). *Proceedings of the Royal Society of London A*. **452** (1954): 2551–2577. arXiv:quant-ph/9601029 (https://arxiv.org/abs/quant-ph/9601029). Bibcode:1996RSPSA.452.2551S (https://ui.adsabs.harvard.edu/abs/1996RSPSA.452.2551S). doi:10.1098/rspa.1996.0136 (https://doi.org/10.1098%2Frspa.1996.0136). S2CID 8246615 (https://api.semanticscholar.org/CorpusID:8246615). Archived from the original (http://www.citebase.org/cgi-bin/citations?id=oai:arXiv.org:quant-ph/9601029) on May 19, 2006. Retrieved April 5, 2020.
30. DiVincenzo, David P. (1996). "Topics in Quantum Computers". arXiv:cond-mat/9612126 (https://arxiv.org/abs/cond-mat/9612126). Bibcode:1996cond.mat.12126D (https://ui.adsabs.harvard.edu/abs/1996cond.mat.12126D).
31. Kitaev, A. Yu (2003). "Fault-tolerant quantum computation by anyons". *Annals of Physics*. **303** (1): 2–30. arXiv:quant-ph/9707021 (https://arxiv.org/abs/quant-ph/9707021). Bibcode:2003AnPhy.303....2K (https://ui.adsabs.harvard.edu/abs/2003AnPhy.303....2K). doi:10.1016/S0003-4916(02)00018-0 (https://doi.org/10.1016%2FS0003-4916%2802%2900018-0). S2CID 119087885 (https://api.semanticscholar.org/CorpusID:119087885).
32. Loss, Daniel; DiVincenzo, David P. (January 1, 1998). "Quantum Computation with Quantum Dots". *Physical Review A*. **57** (1): 120–126. arXiv:cond-mat/9701055 (https://arxiv.org/abs/cond-mat/9701055). Bibcode:1998PhRvA..57..120L (https://ui.adsabs.harvard.edu/abs/1998PhRvA..57..120L). doi:10.1103/PhysRevA.57.120 (https://doi.org/10.1103%2FPhysRevA.57.120). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 13152124 (https://api.semanticscholar.org/CorpusID:13152124).
33. Chuang, Isaac L.; Gershenfeld, Neil; Kubinec, Mark (April 13, 1998). "Experimental Implementation of Fast Quantum Searching". *Physical Review Letters*. **80** (15): 3408–3411. Bibcode:1998PhRvL..80.3408C (https://ui.adsabs.harvard.edu/abs/1998PhRvL..80.3408C). doi:10.1103/PhysRevLett.80.3408 (https://doi.org/10.1103%2FPhysRevLett.80.3408). S2CID 13891055 (https://api.semanticscholar.org/CorpusID:13891055).

34. Kane, B. E. (May 14, 1998). "A silicon-based nuclear spin quantum computer". *Nature*. **393** (6681): 133–137. Bibcode:1998Natur.393..133K (https://ui.adsabs.harvard.edu/abs/1998Natur.393..133K). doi:10.1038/30156 (https://doi.org/10.1038%2F30156). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). S2CID 8470520 (https://api.semanticscholar.org/CorpusID:8470520).
35. Chuang, Isaac L.; Gershenfeld, Neil; Kubinec, Markdoi (April 1998). "Experimental Implementation of Fast Quantum Searching" (https://link.aps.org/doi/10.1103/PhysRevLett.80.3408). *Physical Review Letters*. **80** (15). American Physical Society: 3408–3411. Bibcode:1998PhRvL..80.3408C (https://ui.adsabs.harvard.edu/abs/1998PhRvL..80.3408C). doi:10.1103/PhysRevLett.80.3408 (https://doi.org/10.1103%2FPhysRevLett.80.3408).
36. "Hidetoshi Nishimori – Applying quantum annealing to computers" (https://www.titech.ac.jp/english/public-relations/research/stories/faces13-nishimori). *Tokyo Institute of Technology*. Retrieved September 8, 2022.
37. Gottesman, Daniel (1999). "The Heisenberg Representation of Quantum Computers". In Corney, S. P.; Delbourgo, R.; Jarvis, P. D. (eds.). *Proceedings of the Xxii International Colloquium on Group Theoretical Methods in Physics*. Vol. 22. Cambridge, Massachusetts: International Press. pp. 32–43. arXiv:quant-ph/9807006v1 (https://arxiv.org/abs/quant-ph/9807006v1). Bibcode:1998quant.ph..7006G (https://ui.adsabs.harvard.edu/abs/1998quant.ph..7006G).
38. Braunstein, S. L.; Caves, C. M.; Jozsa, R.; Linden, N.; Popescu, S.; Schack, R. (1999). "Separability of Very Noisy Mixed States and Implications for NMR Quantum Computing". *Physical Review Letters*. **83** (5): 1054–1057. arXiv:quant-ph/9811018 (https://arxiv.org/abs/quant-ph/9811018). Bibcode:1999PhRvL..83.1054B (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83.1054B). doi:10.1103/PhysRevLett.83.1054 (https://doi.org/10.1103%2FPhysRevLett.83.1054). S2CID 14429986 (https://api.semanticscholar.org/CorpusID:14429986).
39. Nakamura, Y.; Pashkin, Yu A.; Tsai, J. S. (April 1999). "Coherent control of macroscopic quantum states in a single-Cooper-pair box" (https://www.nature.com/articles/19718). *Nature*. **398** (6730): 786–788. arXiv:cond-mat/9904003 (https://arxiv.org/abs/cond-mat/9904003). Bibcode:1999Natur.398..786N (https://ui.adsabs.harvard.edu/abs/1999Natur.398..786N). doi:10.1038/19718 (https://doi.org/10.1038%2F19718). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). S2CID 4392755 (https://api.semanticscholar.org/CorpusID:4392755).
40. Linden, Noah; Popescu, Sandu (2001). "Good Dynamics versus Bad Kinematics: Is Entanglement Needed for Quantum Computation?". *Physical Review Letters*. **87** (4): 047901. arXiv:quant-ph/9906008 (https://arxiv.org/abs/quant-ph/9906008). Bibcode:2001PhRvL..87d7901L (https://ui.adsabs.harvard.edu/abs/2001PhRvL..87d7901L). doi:10.1103/PhysRevLett.87.047901 (https://doi.org/10.1103%2FPhysRevLett.87.047901). PMID 11461646 (https://pubmed.ncbi.nlm.nih.gov/11461646). S2CID 10533287 (https://api.semanticscholar.org/CorpusID:10533287).
41. Raussendorf, R.; Briegel, H. J. (2001). "A One-Way Quantum Computer". *Physical Review Letters*. **86** (22): 5188–91. Bibcode:2001PhRvL..86.5188R (https://ui.adsabs.harvard.edu/abs/2001PhRvL..86.5188R). CiteSeerX 10.1.1.252.5345 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.252.5345). doi:10.1103/PhysRevLett.86.5188 (https://doi.org/10.1103%2FPhysRevLett.86.5188). PMID 11384453 (https://pubmed.ncbi.nlm.nih.gov/11384453).
42. n.d. Institute for Quantum Computing (http://www.iqc.ca) "Quick Facts" (https://web.archive.org/web/20190507063322/https://uwaterloo.ca/institute-for-quantum-computing/about/quick-facts). May 15, 2013. Archived from the original (https://uwaterloo.ca/institute-for-quantum-computing/about/quick-facts) on May 7, 2019. Retrieved July 26, 2016.

43. Dumke, R.; Volk, M.; Müther, T.; Buchkremer, F. B. J.; Birkl, G.; Ertmer, W. (August 8, 2002). "Micro-optical Realization of Arrays of Selectively Addressable Dipole Traps: A Scalable Configuration for Quantum Computation with Atomic Qubits" (https://link.aps.org/doi/10.1103/PhysRevLett.89.097903). *Physical Review Letters*. **89** (9): 097903. arXiv:quant-ph/0110140 (https://arxiv.org/abs/quant-ph/0110140). Bibcode:2002PhRvL..89i7903D (https://ui.adsabs.harvard.edu/abs/2002PhRvL..89i7903D). doi:10.1103/PhysRevLett.89.097903 (https://doi.org/10.1103%2FPhysRevLett.89.097903). PMID 12190441 (https://pubmed.ncbi.nlm.nih.gov/12190441).
44. Gulde, S.; Riebe, M.; Lancaster, G. P. T.; Becher, C.; Eschner, J.; Häffner, H.; Schmidt-Kaler, F.; Chuang, I. L.; Blatt, R. (January 2, 2003). "Implementation of the Deutsch–Jozsa algorithm on an ion-trap quantum computer". *Nature*. **421** (6918): 48–50. Bibcode:2003Natur.421...48G (https://ui.adsabs.harvard.edu/abs/2003Natur.421...48G). doi:10.1038/nature01336 (https://doi.org/10.1038%2Fnature01336). PMID 12511949 (https://pubmed.ncbi.nlm.nih.gov/12511949). S2CID 4401708 (https://api.semanticscholar.org/CorpusID:4401708).
45. Pittman, T. B.; Fitch, M. J.; Jacobs, B. C.; Franson, J. D. (2003). "Experimental controlled-not logic gate for single photons in the coincidence basis". *Physical Review A*. **68** (3): 032316. arXiv:quant-ph/0303095 (https://arxiv.org/abs/quant-ph/0303095). Bibcode:2003PhRvA..68c2316P (https://ui.adsabs.harvard.edu/abs/2003PhRvA..68c2316P). doi:10.1103/physreva.68.032316 (https://doi.org/10.1103%2Fphysreva.68.032316). S2CID 119476903 (https://api.semanticscholar.org/CorpusID:119476903).
46. O'Brien, J. L.; Pryde, G. J.; White, A. G.; Ralph, T. C.; Branning, D. (2003). "Demonstration of an all-optical quantum controlled-NOT gate". *Nature*. **426** (6964): 264–267. arXiv:quant-ph/0403062 (https://arxiv.org/abs/quant-ph/0403062). Bibcode:2003Natur.426..264O (https://ui.adsabs.harvard.edu/abs/2003Natur.426..264O). doi:10.1038/nature02054 (https://doi.org/10.1038%2Fnature02054). PMID 14628045 (https://pubmed.ncbi.nlm.nih.gov/14628045). S2CID 9883628 (https://api.semanticscholar.org/CorpusID:9883628).
47. Schmidt-Kaler, F.; Häffner, H.; Riebe, M.; Gulde, S.; Lancaster, G. P. T.; Deutschle, T.; Becher, C.; Roos, C. F.; Eschner, J.; Blatt, R. (March 27, 2003). "Realization of the Cirac-Zoller controlled-NOT quantum gate". *Nature*. **422** (6930): 408–411. Bibcode:2003Natur.422..408S (https://ui.adsabs.harvard.edu/abs/2003Natur.422..408S). doi:10.1038/nature01494 (https://doi.org/10.1038%2Fnature01494). PMID 12660777 (https://pubmed.ncbi.nlm.nih.gov/12660777). S2CID 4401898 (https://api.semanticscholar.org/CorpusID:4401898).
48. Riebe, M.; Häffner, H.; Roos, C. F.; Hänsel, W.; Benhelm, J.; Lancaster, G. P. T.; Körber, T. W.; Becher, C.; Schmidt-Kaler, F.; James, D. F. V.; Blatt, R. (June 17, 2004). "Deterministic quantum teleportation with atoms". *Nature*. **429** (6993): 734–737. Bibcode:2004Natur.429..734R (https://ui.adsabs.harvard.edu/abs/2004Natur.429..734R). doi:10.1038/nature02570 (https://doi.org/10.1038%2Fnature02570). PMID 15201903 (https://pubmed.ncbi.nlm.nih.gov/15201903). S2CID 4397716 (https://api.semanticscholar.org/CorpusID:4397716).
49. Zhao, Z.; Chen, Y. A.; Zhang, A. N.; Yang, T.; Briegel, H. J.; Pan, J. W. (2004). "Experimental demonstration of five-photon entanglement and open-destination teleportation". *Nature*. **430** (6995): 54–58. arXiv:quant-ph/0402096 (https://arxiv.org/abs/quant-ph/0402096). Bibcode:2004Natur.430...54Z (https://ui.adsabs.harvard.edu/abs/2004Natur.430...54Z). doi:10.1038/nature02643 (https://doi.org/10.1038%2Fnature02643). PMID 15229594 (https://pubmed.ncbi.nlm.nih.gov/15229594). S2CID 4336020 (https://api.semanticscholar.org/CorpusID:4336020).
50. Dumé, Belle (November 22, 2005). "Breakthrough for quantum measurement" (https://physicsworld.com/a/breakthrough-for-quantum-measurement/). PhysicsWeb. Retrieved August 10, 2018.

51. Häffner, H.; Hänsel, W.; Roos, C. F.; Benhelm, J.; Chek-Al-Kar, D.; Chwalla, M.; Körber, T.; Rapol, U. D.; Riebe, M.; Schmidt, P. O.; Becher, C.; Gühne, O.; Dür, W.; Blatt, R. (December 1, 2005). "Scalable multiparticle entanglement of trapped ions". *Nature*. **438** (7068): 643–646. arXiv:quant-ph/0603217 (https://arxiv.org/abs/quant-ph/0603217). Bibcode:2005Natur.438..643H (https://ui.adsabs.harvard.edu/abs/2005Natur.438..643H). doi:10.1038/nature04279 (https://doi.org/10.1038%2Fnature04279). PMID 16319886 (https://pubmed.ncbi.nlm.nih.gov/16319886). S2CID 4411480 (https://api.semanticscholar.org/CorpusID:4411480).
52. "Bang-bang: a step closer to quantum supercomputers" (https://web.archive.org/web/20180830005255/http://www.admin.ox.ac.uk/po/news/2005-06/jan/04a.shtml). England: University of Oxford. January 4, 2006. Archived from the original (http://www.admin.ox.ac.uk/po/news/2005-06/jan/04a.shtml) on August 30, 2018. Retrieved December 29, 2007.
53. Dowling, Jonathan P. (2006). "To Compute or Not to Compute?" (https://doi.org/10.1038%2F439919a). *Nature*. **439** (7079): 919–920. Bibcode:2006Natur.439..919D (https://ui.adsabs.harvard.edu/abs/2006Natur.439..919D). doi:10.1038/439919a (https://doi.org/10.1038%2F439919a). PMID 16495978 (https://pubmed.ncbi.nlm.nih.gov/16495978). S2CID 4327844 (https://api.semanticscholar.org/CorpusID:4327844).
54. Dumé, Belle (February 23, 2007). "Entanglement heats up" (https://web.archive.org/web/20071019032222/http://physicsworld.com/cws/article/news/24285). *Physics World*. Archived from the original (http://physicsworld.com/cws/article/news/24285) on October 19, 2007.
55. "Captain Kirk's clone and the eavesdropper" (https://web.archive.org/web/20070207105035/http://www.york.ac.uk/admin/presspr/pressreleases/kirkclone.htm) (Press release). England: University of York. February 16, 2006. Archived from the original (http://www.york.ac.uk/admin/presspr/pressreleases/kirkclone.htm) on February 7, 2007. Retrieved December 29, 2007.
56. "Soft Machines – Some personal views on nanotechnology, science and science policy from Richard Jones" (http://www.softmachines.org/wordpress/). June 23, 2023. Retrieved July 5, 2023.
57. Simonite, Tom (June 8, 2010). "Error-check breakthrough in quantum computing" (http://www.newscientisttech.com/article/dn9301-errorcheck-breakthrough-in-quantum-computing.html). *New Scientist*. Retrieved May 20, 2010.
58. "12-qubits Reached In Quantum Information Quest" (https://www.sciencedaily.com/releases/2006/05/060508164700.htm). *ScienceDaily*. May 8, 2006. Retrieved May 20, 2010.
59. Simonite, Tom (July 7, 2010). "Flat 'ion trap' holds quantum computing promise" (http://www.newscientisttech.com/article/dn9502-flat-ion-trap-holds-quantum-computing-promise.html). *New Scientist*. Retrieved May 20, 2010.
60. Luerweg, Frank (July 12, 2006). "Quantum Computer: Laser tweezers sort atoms" (https://web.archive.org/web/20071215041757/http://www.physorg.com/news71935118.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news71935118.html) on December 15, 2007. Retrieved December 29, 2007.
61. " 'Electron-spin' trick boosts quantum computing" (https://web.archive.org/web/20061122102719/http://www.newscientisttech.com/article.ns?id=dn9768). *New Scientist*. August 16, 2006. Archived from the original (http://www.newscientisttech.com/article.ns?id=dn9768) on November 22, 2006. Retrieved December 29, 2007.
62. Berger, Michael (August 16, 2006). "Quantum Dot Molecules – One Step Further Towards Quantum Computing" (http://www.newswiretoday.com/news/7723/). *Newswire Today*. Retrieved December 29, 2007.
63. "Spinning new theory on particle spin brings science closer to quantum computing" (https://web.archive.org/web/20080117223659/http://www.physorg.com/news76863086.html). *PhysOrg.com*. September 7, 2006. Archived from the original (http://www.physorg.com/news76863086.html) on January 17, 2008. Retrieved December 29, 2007.

64. Merali, Zeeya (October 4, 2006). "Spooky steps to a quantum network" (http://www.newscientisttech.com/article/dn10226-spooky-steps-to-a-quantum-network.html). *New Scientist*. **192** (2572): 12. doi:10.1016/s0262-4079(06)60639-8 (https://doi.org/10.1016%2Fs0262-4079%2806%2960639-8). Retrieved December 29, 2007.
65. Zyga, Lisa (October 24, 2006). "Scientists present method for entangling macroscopic objects" (https://web.archive.org/web/20071013014512/http://physorg.com/news80896839.html). *PhysOrg.com*. Archived from the original (http://physorg.com/news80896839.html) on October 13, 2007. Retrieved December 29, 2007.
66. Kloeppel, James E. (November 2, 2006). "Quantum coherence possible in incommensurate electronic systems" (http://news.illinois.edu/news/06/1102quantum.html). Champaign-Urbana, Illinois: University of Illinois. Retrieved August 19, 2010.
67. "A Quantum (Computer) Step: Study Shows It's Feasible to Read Data Stored as Nuclear 'Spins' " (https://web.archive.org/web/20070929120422/http://physorg.com/news83163617.html). *PhysOrg.com*. November 19, 2006. Archived from the original (http://physorg.com/news83163617.html) on September 29, 2007. Retrieved December 29, 2007.
68. Hecht, Jeff (January 8, 2007). "Nanoscopic 'coaxial cable' transmits light" (http://www.newscientisttech.com/article/dn10911-nanoscopic-coaxial-cable-transmits-light.html). *New Scientist*. Retrieved December 30, 2007.
69. "Toshiba unveils quantum security" (https://web.archive.org/web/20070304090639/http://www.e4engineering.com/Articles/298360/Toshiba+unveils+quantum+security.htm). *The Engineer*. February 21, 2007. Archived from the original (http://www.e4engineering.com/Articles/298360/Toshiba+unveils+quantum+security.htm) on March 4, 2007. Retrieved December 30, 2007.
70. Lu, Chao-Yang; Zhou, Xiao-Qi; Gühne, Otfried; Gao, Wei-Bo; Zhang, Jin; Yuan, Zhen-Sheng; Goebel, Alexander; Yang, Tao; Pan, Jian-Wei (2007). "Experimental entanglement of six photons in graph states". *Nature Physics*. **3** (2): 91–95. arXiv:quant-ph/0609130 (https://arxiv.org/abs/quant-ph/0609130). Bibcode:2007NatPh...3...91L (https://ui.adsabs.harvard.edu/abs/2007NatPh...3...91L). doi:10.1038/nphys507 (https://doi.org/10.1038%2Fnphys507). S2CID 16319327 (https://api.semanticscholar.org/CorpusID:16319327).
71. Danos, V.; Kashefi, E.; Panangaden, P. (2007). "The measurement calculus". *Journal of the Association for Computing Machinery*. **54** (2): 8. arXiv:0704.1263 (https://arxiv.org/abs/0704.1263). doi:10.1145/1219092.1219096 (https://doi.org/10.1145%2F1219092.1219096). S2CID 5851623 (https://api.semanticscholar.org/CorpusID:5851623).
72. Marquit, Miranda (April 18, 2007). "First use of Deutsch's Algorithm in a cluster state quantum computer" (https://web.archive.org/web/20080117224207/http://www.physorg.com/news96107220.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news96107220.html) on January 17, 2008. Retrieved December 30, 2007.
73. Zeeya Merali (March 15, 2007). "The universe is a string-net liquid" (https://www.newscientist.com/article.ns?id=mg19325954.200&feedId=fundamentals_rss20). *New Scientist*. Retrieved December 30, 2007.
74. "A Single-Photon Server with Just One Atom" (http://www.mpg.de/english/illustrationsDocumentation/documentation/pressReleases/2007/pressRelease200703091/index.html) (Press release). Max Planck Society. March 12, 2007. Retrieved December 30, 2007.
75. Steve Bush (April 19, 2007). "Cambridge team closer to working quantum computer" (https://archive.today/20120515222358/http://www.electronicsweekly.com/Articles/2007/04/19/41206/Cambridge+team+closer+to+working+quantum+computer.htm). *Electronics Weekly*. Archived from the original (http://www.electronicsweekly.com/Articles/2007/04/19/41206/Cambridge+team+closer+to+working+quantum+computer.htm) on May 15, 2012. Retrieved December 30, 2007.

76. Farivar, Cyrus (May 7, 2007). "It's the "Wiring" That's Tricky in Quantum Computing" (https://web.archive.org/web/20080706171401/http://www.wired.com/science/discoveries/news/2007/05/quantumcoupling). *Wired*. Archived from the original (https://www.wired.com/science/discoveries/news/2007/05/quantumcoupling) on July 6, 2008. Retrieved December 30, 2007.
77. "NEC, JST, and RIKEN Successfully Demonstrate World's First Controllably Coupled Qubits" (http://media-newswire.com/release_1049194.html) (Press release). Media-Newswire.com. May 8, 2007. Retrieved December 30, 2007.
78. Minkel, J. R. (May 16, 2007). "Spintronics Breaks the Silicon Barrier" (http://www.sciam.com/article.cfm?articleId=959FBD96-E7F2-99DF-341F959A7DA2A292&chanId=sa013&modsrc=most_popular). *Scientific American*. Retrieved December 30, 2007.
79. Zyga, Lisa (May 22, 2007). "Scientists demonstrate quantum state exchange between light and matter" (https://web.archive.org/web/20080307093926/http://www.physorg.com/news99050442.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news99050442.html) on March 7, 2008. Retrieved December 30, 2007.
80. Dutt, M. V.; Childress, L.; Jiang, L.; Togan, E.; Maze, J.; Jelezko, F.; Zibrov, A. S.; Hemmer, P. R; Lukin, M. D. (June 1, 2007). "Quantum Register Based on Individual Electronic and Nuclear Spin Qubits in Diamond". *Science*. **316** (5829): 1312–1316. Bibcode:2007Sci...316.....D (https://ui.adsabs.harvard.edu/abs/2007Sci...316.....D). doi:10.1126/science.1139831 (https://doi.org/10.1126%2Fscience.1139831). PMID 17540898 (https://pubmed.ncbi.nlm.nih.gov/17540898). S2CID 20697722 (https://api.semanticscholar.org/CorpusID:20697722).
81. Plantenberg, J. H.; De Groot, P. C.; Harmans, C. J. P. M.; Mooij, J. E. (June 14, 2007). "Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits". *Nature*. **447** (7146): 836–839. Bibcode:2007Natur.447..836P (https://ui.adsabs.harvard.edu/abs/2007Natur.447..836P). doi:10.1038/nature05896 (https://doi.org/10.1038%2Fnature05896). PMID 17568742 (https://pubmed.ncbi.nlm.nih.gov/17568742). S2CID 3054763 (https://api.semanticscholar.org/CorpusID:3054763).
82. Inman, Mason (June 17, 2007). "Atom trap is a step towards a quantum computer" (http://www.newscientisttech.com/article/dn12082-atom-trap-is-a-step-towards-a-quantum-computer-.html). *New Scientist*. Retrieved December 30, 2007.
83. "Nanotechnology and Emerging Technologies News from Nanowerk" (https://www.nanowerk.com/). *www.nanowerk.com*. Retrieved July 5, 2023.
84. "Discovery Of 'Hidden' Quantum Order Improves Prospects For Quantum Super Computers" (https://www.sciencedaily.com/releases/2007/07/070726142010.htm). *Science Daily*. July 27, 2007. Retrieved December 30, 2007.
85. Marquit, Miranda (July 23, 2007). "Indium arsenide may provide clues to quantum information processing" (https://web.archive.org/web/20070926220146/http://www.physorg.com/news104418332.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news104418332.html) on September 26, 2007. Retrieved December 30, 2007.
86. "Thousands of Atoms Swap 'Spins' with Partners in Quantum Square Dance" (https://web.archive.org/web/20071218224341/http://www.nist.gov/public_affairs/releases/quantum_gate.html). *National Institute of Standards and Technology*. July 25, 2007. Archived from the original (https://www.nist.gov/public_affairs/releases/quantum_gate.html) on December 18, 2007. Retrieved December 30, 2007.
87. Zyga, Lisa (August 15, 2007). "Ultrafast quantum computer uses optically controlled electrons" (https://web.archive.org/web/20080102004025/http://www.physorg.com/news106395871.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news106395871.html) on January 2, 2008. Retrieved December 30, 2007.
88. Bush, Steve (August 15, 2007). "Research points way to qubits on standard chips" (http://www.electronicsweekly.com/Articles/2007/08/15/41988/research-points-way-to-qubits-on-standard-chips.htm). *Electronics Weekly*. Retrieved December 30, 2007.

89. "Computing Breakthrough Could Elevate Security To Unprecedented Levels" (https://www.sciencedaily.com/releases/2007/08/070816143801.htm). *ScienceDaily*. August 17, 2007. Retrieved December 30, 2007.
90. Battersby, Stephen (August 21, 2007). "Blueprints drawn up for quantum computer RAM" (https://www.newscientist.com/article/dn12516-blueprints-drawn-up-for-quantum-computer-ram.html). *New Scientist*. Retrieved December 30, 2007.
91. "Photon-transistors for the supercomputers of the future" (https://web.archive.org/web/20080101165713/http://physorg.com/news107357370.html). *PhysOrg.com*. August 26, 2007. Archived from the original (http://physorg.com/news107357370.html) on January 1, 2008. Retrieved December 30, 2007.
92. "Physicists establish "spooky" quantum communication" (https://web.archive.org/web/20071228220630/http://www.ns.umich.edu/htdocs/releases/story.php?id=6016). University of Michigan. September 5, 2007. Archived from the original (http://www.ns.umich.edu/htdocs/releases/story.php?id=6016) on December 28, 2007. Retrieved December 30, 2007.
93. huliq.com (http://www.huliq.com) "Qubits poised to reveal our secrets" (http://www.huliq.com/34160/qubits-poised-to-reveal-our-secrets). September 13, 2007. Retrieved December 30, 2007.
94. Das, Saswato (September 26, 2007). "Quantum chip rides on superconducting bus" (https://www.newscientist.com/article/dn12696-quantum-chip-rides-on-superconducting-bus.html). *New Scientist*. Retrieved December 30, 2007.
95. "Superconducting Quantum Computing Cable Created" (https://www.sciencedaily.com/releases/2007/09/070926172232.htm). *ScienceDaily*. September 27, 2007. Retrieved December 30, 2007.
96. Bush, Steve (October 11, 2007). "Qubit transmission signals quantum computing advance" (https://web.archive.org/web/20071012144831/http://www.electronicsweekly.com/Articles/2007/10/11/42346/qubit+transmission+signals+quantum+computing+advance.htm). *Electronics Weekly*. Archived from the original (http://www.electronicsweekly.com/Articles/2007/10/11/42346/qubit+transmission+signals+quantum+computing+advance.htm) on October 12, 2007. Retrieved December 30, 2007.
97. Hodgin, Rick C. (October 8, 2007). "New material breakthrough brings quantum computers one step closer" (https://web.archive.org/web/20071212162540/http://www.tgdaily.com/content/view/34244/113/). *TG Daily*. Archived from the original (http://www.tgdaily.com/content/view/34244/113/) on December 12, 2007. Retrieved December 30, 2007.
98. "Single electron-spin memory with a semiconductor quantum dot" (http://optics.org/cws/article/journals/31503). *Optics.org*. October 19, 2007. Retrieved December 30, 2007.
99. Battersby, Stephen (November 7, 2007). " 'Light trap' is a step towards quantum memory" (https://www.newscientist.com/channel/fundamentals/quantum-world/dn12887-light-trap-is-a-step-towards-quantum-memory-.html). *New Scientist*. Retrieved December 30, 2007.
100. "World's First 28 qubit Quantum Computer Demonstrated Online at Supercomputing 2007 Conference" (https://web.archive.org/web/20180830041346/https://www.nanowerk.com/news/newsid=3274.php). *Nanowerk.com*. November 12, 2007. Archived from the original (http://www.nanowerk.com/news/newsid=3274.php) on August 30, 2018. Retrieved December 30, 2007.
101. "Desktop device generates and traps rare ultracold molecules" (https://web.archive.org/web/20071215075835/http://www.physorg.com/news116696579.html). *PhysOrg.com*. December 12, 2007. Archived from the original (http://www.physorg.com/news116696579.html) on December 15, 2007. Retrieved December 31, 2007.
102. Luke, Kim (December 19, 2007). "U of T scientists make quantum computing leap Research is step toward building first quantum computers" (https://web.archive.org/web/20071228170511/http://www.news.utoronto.ca/bin6/071219-3563.asp). University of Toronto. Archived from the original (http://www.news.utoronto.ca/bin6/071219-3563.asp) on December 28, 2007. Retrieved December 31, 2007.

103. Trauzettel, Björn; Bulaev, Denis V.; Loss, Daniel; Burkard, Guido (February 18, 2007). "Spin qubits in graphene quantum dots". *Nature Physics*. **3** (3): 192–196. arXiv:cond-mat/0611252 (https://arxiv.org/abs/cond-mat/0611252). Bibcode:2007NatPh...3..192T (https://ui.adsabs.harvard.edu/abs/2007NatPh...3..192T). doi:10.1038/nphys544 (https://doi.org/10.1038%2Fnphys544). S2CID 119431314 (https://api.semanticscholar.org/CorpusID:119431314).
104. Harrow, Aram W; Hassidim, Avinatan; Lloyd, Seth (2008). "Quantum algorithm for solving linear systems of equations". *Physical Review Letters*. **103** (15): 150502. arXiv:0811.3171 (https://arxiv.org/abs/0811.3171). Bibcode:2009PhRvL.103o0502H (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103o0502H). doi:10.1103/PhysRevLett.103.150502 (https://doi.org/10.1103%2FPhysRevLett.103.150502). PMID 19905613 (https://pubmed.ncbi.nlm.nih.gov/19905613). S2CID 5187993 (https://api.semanticscholar.org/CorpusID:5187993).
105. Marquit, Miranda (January 15, 2008). "Graphene quantum dot may solve some quantum computing problems" (https://web.archive.org/web/20080117230333/http://www.physorg.com/news119632225.html). Archived from the original (http://www.physorg.com/news119632225.html) on January 17, 2008. Retrieved January 16, 2008.
106. "Scientists succeed in storing quantum bit" (http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=205918527). *EE Times Europe*. January 25, 2008. Retrieved February 5, 2008.
107. Zyga, Lisa (February 26, 2008). "Physicists demonstrate qubit-qutrit entanglement" (https://web.archive.org/web/20080229001836/http://www.physorg.com/news123244300.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news123244300.html) on February 29, 2008. Retrieved February 27, 2008.
108. "Analog logic for quantum computing" (https://www.sciencedaily.com/releases/2008/02/080221101910.htm). *ScienceDaily*. February 26, 2008. Retrieved February 27, 2008.
109. Kotala, Zenaida Gonzalez (March 5, 2008). "Future 'quantum computers' will offer increased efficiency... and risks" (http://www.eurekalert.org/pub_releases/2008-03/uocf-fc030508.php). *Eurekalert.org*. Retrieved March 5, 2008.
110. Kurzweil, Ray (March 6, 2008). "Entangled memory is a first" (http://www.kurzweilai.net/news/frame.html?main=news_single.html?id%3D8142). Retrieved March 8, 2008.
111. Fryer, Joann (March 27, 2008). "Silicon chips for optical quantum technologies" (http://www.eurekalert.org/pub_releases/2008-03/uob-scf032608.php). *Eurekalert.org*. Retrieved March 29, 2008.
112. Kurzweil, Ray (April 7, 2008). "Qutrit breakthrough brings quantum computers closer" (http://www.kurzweilai.net/news/frame.html?main=news_single.html?id%3D8354). Retrieved April 7, 2008.
113. Greene, Kate (April 15, 2008). "Toward a quantum internet" (http://www.technologyreview.com/Infotech/20565/?a=f). *Technology Review*. Retrieved April 16, 2008.
114. "Scientists discover exotic quantum state of matter" (https://web.archive.org/web/20080430131534/http://physorg.com/news128261028.html). Princeton University. April 24, 2008. Archived from the original (http://physorg.com/news128261028.html) on April 30, 2008. Retrieved April 29, 2008.
115. Dumé, Belle (May 23, 2008). "Spin states endure in quantum dot" (https://web.archive.org/web/20080529004841/http://physicsworld.com/cws/article/news/34359). *Physics World*. Archived from the original (http://physicsworld.com/cws/article/news/34359) on May 29, 2008. Retrieved June 3, 2008.
116. Lee, Chris (May 27, 2008). "Molecular magnets in soap bubbles could lead to quantum RAM" (https://arstechnica.com/news.ars/post/20080527-molecular-magnets-in-soap-bubbles-could-lead-to-quantum-ram.html). *ARSTechnica*. Retrieved June 3, 2008.
117. Weizmann Institute of Science (June 2, 2008). "Scientists find new 'quasiparticles' " (http://physorg.com/news131631206.html). *PhysOrg.com*. Retrieved June 3, 2008.

118. Zyga, Lisa (June 23, 2008). "Physicists Store Images in Vapor" (https://web.archive.org/web/20080915130750/http://www.physorg.com/news133439288.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news133439288.html) on September 15, 2008. Retrieved June 26, 2008.
119. "Physicists Produce Quantum-Entangled Images" (https://web.archive.org/web/20080829225636/http://www.physorg.com/news133624014.html). *PhysOrg.com*. June 25, 2008. Archived from the original (http://www.physorg.com/news133624014.html) on August 29, 2008. Retrieved June 26, 2008.
120. Tally, Steve (June 26, 2008). "Quantum computing breakthrough arises from unknown molecule" (https://web.archive.org/web/20190202103204/https://news.uns.purdue.edu/x/2008a/080626KlimeckArsenic.html). Purdue University. Archived from the original (http://news.uns.purdue.edu/x/2008a/080626KlimeckArsenic.html) on February 2, 2019. Retrieved June 28, 2008.
121. Rugani, Lauren (July 17, 2008). "Quantum Leap" (http://www.technologyreview.com/Infotech/21086/). *Technology Review*. Retrieved July 17, 2008.
122. "Breakthrough In Quantum Mechanics: Superconducting Electronic Circuit Pumps Microwave Photons" (https://www.sciencedaily.com/releases/2008/08/080805150812.htm). *ScienceDaily*. August 5, 2008. Retrieved August 6, 2008.
123. "New probe could aid quantum computing" (https://web.archive.org/web/20080905193420/http://www.physorg.com/news139665168.html). *PhysOrg.com*. September 3, 2008. Archived from the original (http://www.physorg.com/news139665168.html) on September 5, 2008. Retrieved September 6, 2008.
124. "Novel Process Promises To Kick-start Quantum Technology Sector" (https://www.sciencedaily.com/releases/2008/09/080925144609.htm). *ScienceDaily*. September 25, 2008. Retrieved October 16, 2008.
125. O'Brien, Jeremy L. (September 22, 2008). "Quantum computing over the rainbow" (http://physics.aps.org/articles/v1/23). Retrieved October 16, 2008.
126. "Relationships Between Quantum Dots – Stability and Reproduction" (https://web.archive.org/web/20081022201107/http://www.scienceblog.com/cms/blog/624-relationships-between-quantum-dots-stability-and-reproduction-17599.html). *Science Blog*. October 20, 2008. Archived from the original (http://www.scienceblog.com/cms/blog/624-relationships-between-quantum-dots-stability-and-reproduction-17599.html) on October 22, 2008. Retrieved October 20, 2008.
127. Schultz, Steven (October 22, 2008). "Memoirs of a qubit: Hybrid memory solves key problem for quantum computing" (http://www.eurekalert.org/pub_releases/2008-10/pues-smt102208.php). *Eurekalert.com*. Retrieved October 23, 2008.
128. "World's Smallest Storage Space ... the Nucleus of an Atom" (https://www.nsf.gov/news/news_summ.jsp?cntn_id=112538&govDel=USNSF_51). *National Science Foundation News*. October 23, 2008. Retrieved October 27, 2008.
129. Stober, Dan (November 20, 2008). "Stanford: Quantum computing spins closer" (http://www.eurekalert.org/pub_releases/2008-11/su-sqc112008.php). *Eurekalert.com*. Retrieved November 22, 2008.
130. Marquit, Miranda (December 5, 2008). "Quantum computing: Entanglement may not be necessary" (https://web.archive.org/web/20081208091811/http://www.physorg.com/news147698804.html). *PhysOrg.com*. Archived from the original (http://www.physorg.com/news147698804.html) on December 8, 2008. Retrieved December 9, 2008.
131. "Dwave System's 128 qubit chip has been made" (https://web.archive.org/web/20081223060355/http://nextbigfuture.com/2008/12/dwave-systems-128-qubit-chip-has-been.html). *Next Big Future*. December 19, 2008. Archived from the original (http://nextbigfuture.com/2008/12/dwave-systems-128-qubit-chip-has-been.html) on December 23, 2008. Retrieved December 20, 2008.

132. "Three Times Higher Carbon 12 Purity for Synthetic Diamond Enables Better Quantum Computing" (https://web.archive.org/web/20090411055856/http://nextbigfuture.com/2009/04/element-six-is-global-leader-europe.html). *Next Big Future*. April 7, 2009. Archived from the original (http://nextbigfuture.com/2009/04/element-six-is-global-leader-europe.html) on April 11, 2009. Retrieved May 19, 2009.
133. Greene, Kate (April 23, 2009). "Extending the Life of Quantum Bits" (https://www.technologyreview.com/2009/04/23/213539/extending-the-life-of-quantum-bits/). *Technology Review*. Retrieved June 1, 2020.
134. "Researchers make breakthrough in the quantum control of light" (https://archive.today/20130131221049/http://www.physorg.com/news162814379.html). *PhysOrg.com*. May 29, 2009. Archived from the original (http://www.physorg.com/news162814379.html) on January 31, 2013. Retrieved May 30, 2009.
135. "Physicists demonstrate quantum entanglement in mechanical system" (https://archive.today/20130131084441/http://www.physorg.com/news163253992.html). *PhysOrg.com*. June 3, 2009. Archived from the original (http://www.physorg.com/news163253992.html) on January 31, 2013. Retrieved June 13, 2009.
136. Moore, Nicole Casai (June 24, 2009). "Lasers can lengthen quantum bit memory by 1,000 times" (http://www.eurekalert.org/pub_releases/2009-06/uom-lcl062309.php). *Eurekalert.com*. Retrieved June 27, 2009.
137. "First Electronic Quantum Processor Created" (https://www.sciencedaily.com/releases/2009/06/090628171949.htm). *ScienceDaily*. June 29, 2009. Retrieved June 29, 2009.
138. Lu, C. Y.; Gao, W. B.; Gühne, O.; Zhou, X. Q.; Chen, Z. B.; Pan, J. W. (2009). "Demonstrating Anyonic Fractional Statistics with a Six-Qubit Quantum Simulator". *Physical Review Letters*. **102** (3): 030502. arXiv:0710.0278 (https://arxiv.org/abs/0710.0278). Bibcode:2009PhRvL.102c0502L (https://ui.adsabs.harvard.edu/abs/2009PhRvL.102c0502L). doi:10.1103/PhysRevLett.102.030502 (https://doi.org/10.1103%2FPhysRevLett.102.030502). PMID 19257336 (https://pubmed.ncbi.nlm.nih.gov/19257336). S2CID 11788852 (https://api.semanticscholar.org/CorpusID:11788852).
139. Borghino, Dario (July 6, 2009). "Quantum computer closer: Optical transistor made from single molecule" (http://www.gizmag.com/optical-transistor-made-from-single-molecule/12157/). *Gizmag*. Retrieved July 8, 2009.
140. Johnson, R. Colin (July 8, 2009). "NIST advances quantum computing" (http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=218401022). *EE Times*. Retrieved July 9, 2009.
141. Greene, Kate (August 7, 2009). "Scaling Up a Quantum Computer" (http://www.technologyreview.com/computing/23137/). *Technology Review*. Retrieved August 8, 2009.
142. Devitt, S. J.; Fowler, A. G.; Stephens, A. M.; Greentree, A. D.; Hollenberg, L. C. L.; Munro, W. J.; Nemoto, K. (August 11, 2009). "Architectural design for a topological cluster state quantum computer". *New Journal of Physics*. **11** (83032): 1221. arXiv:0808.1782 (https://arxiv.org/abs/0808.1782). Bibcode:2009NJPh...11h3032D (https://ui.adsabs.harvard.edu/abs/2009NJPh...11h3032D). doi:10.1088/1367-2630/11/8/083032 (https://doi.org/10.1088%2F1367-2630%2F11%2F8%2F083032). S2CID 56195929 (https://api.semanticscholar.org/CorpusID:56195929).
143. Home, J. P.; Hanneke, D.; Jost, J. D.; Amini, J. M.; Leibfried, D.; Wineland, D. J. (September 4, 2009). "Complete Methods Set for Scalable Ion Trap Quantum Information Processing". *Science*. **325** (5945): 1227–1230. arXiv:0907.1865 (https://arxiv.org/abs/0907.1865). Bibcode:2009Sci...325.1227H (https://ui.adsabs.harvard.edu/abs/2009Sci...325.1227H). doi:10.1126/science.1177077 (https://doi.org/10.1126%2Fscience.1177077). PMID 19661380 (https://pubmed.ncbi.nlm.nih.gov/19661380). S2CID 24468918 (https://api.semanticscholar.org/CorpusID:24468918).

144. Politi, A.; Matthews, J. C.; O'Brien, J. L. (2009). "Shor's Quantum Factoring Algorithm on a Photonic Chip". *Science*. **325** (5945): 1221. arXiv:0911.1242 (https://arxiv.org/abs/0911.1242). Bibcode:2009Sci...325.1221P (https://ui.adsabs.harvard.edu/abs/2009Sci...325.1221P). doi:10.1126/science.1173731 (https://doi.org/10.1126%2Fscience.1173731). PMID 19729649 (https://pubmed.ncbi.nlm.nih.gov/19729649). S2CID 17259222 (https://api.semanticscholar.org/CorpusID:17259222).
145. Wesenberg, J. H.; Ardavan, A.; Briggs, G. A. D.; Morton, J. J. L.; Schoelkopf, R. J.; Schuster, D. I.; Mølmer, K. (2009). "Quantum Computing with an Electron Spin Ensemble". *Physical Review Letters*. **103** (7): 070502. arXiv:0903.3506 (https://arxiv.org/abs/0903.3506). Bibcode:2009PhRvL.103g0502W (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103g0502W). doi:10.1103/PhysRevLett.103.070502 (https://doi.org/10.1103%2FPhysRevLett.103.070502). PMID 19792625 (https://pubmed.ncbi.nlm.nih.gov/19792625). S2CID 6990125 (https://api.semanticscholar.org/CorpusID:6990125).
146. Barras, Colin (September 25, 2009). "Photon 'machine gun' could power quantum computers" (https://www.newscientist.com/article/mg20327275.700-photon-machine-gun-could-power-quantum-computers.html?DCMP=OTC-rss&nsref=online-news). *New Scientist*. Retrieved September 26, 2009.
147. November 15, 2009 "First universal programmable quantum computer unveiled" (https://www.newscientist.com/article/dn18154-first-universal-programmable-quantum-computer-unveiled.html). *New Scientist*. November 15, 2009. Retrieved November 16, 2009.
148. "UCSB physicists move 1 step closer to quantum computing" (https://web.archive.org/web/20091123213145/http://www.scienceblog.com/cms/ucsb-physicists-move-1-step-closer-quantum-computing-27431.html). *ScienceBlog*. November 20, 2009. Archived from the original (http://www.scienceblog.com/cms/ucsb-physicists-move-1-step-closer-quantum-computing-27431.html) on November 23, 2009. Retrieved November 23, 2009.
149. Hsu, Jeremy (December 11, 2009). "Google Demonstrates Quantum Algorithm Promising Superfast Search" (http://www.popsci.com/technology/article/2009-12/google-algorithm-uses-quantum-computing-sort-images-faster-ever). Retrieved December 14, 2009.
150. Harris, R.; Brito, F.; Berkley, A. J.; Johansson, J.; Johnson, M. W.; Lanting, T.; Bunyk, P.; Ladizinsky, E.; Bumble, B.; Fung, A.; Kaul, A.; Kleinsasser, A.; Han, S. (2009). "Synchronization of multiple coupled rf-SQUID flux qubits". *New Journal of Physics*. **11** (12): 123022. arXiv:0903.1884 (https://arxiv.org/abs/0903.1884). Bibcode:2009NJPh...11l3022H (https://ui.adsabs.harvard.edu/abs/2009NJPh...11l3022H). doi:10.1088/1367-2630/11/12/123022 (https://doi.org/10.1088%2F1367-2630%2F11%2F12%2F123022). S2CID 54065717 (https://api.semanticscholar.org/CorpusID:54065717).
151. Monz, T.; Kim, K.; Villar, A. S.; Schindler, P.; Chwalla, M.; Riebe, M.; Roos, C. F.; Häffner, H.; Hänsel, W.; Hennrich, M.; Blatt, R (2009). "Realization of Universal Ion Trap Quantum Computation with Decoherence Free Qubits". *Physical Review Letters*. **103** (20): 200503. arXiv:0909.3715 (https://arxiv.org/abs/0909.3715). Bibcode:2009PhRvL.103t0503M (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103t0503M). doi:10.1103/PhysRevLett.103.200503 (https://doi.org/10.1103%2FPhysRevLett.103.200503). PMID 20365970 (https://pubmed.ncbi.nlm.nih.gov/20365970). S2CID 7632319 (https://api.semanticscholar.org/CorpusID:7632319).
152. "A decade of Physics World breakthroughs: 2009 – the first quantum computer" (https://physicsworld.com/a/a-decade-of-physics-world-breakthroughs-2009-the-first-quantum-computer/). *Physics World*. November 29, 2019.
153. January 20, 2010 arXiv blog. "Making Light of Ion Traps" (http://www.technologyreview.com/blog/arxiv/24685/?nlid=2678). Retrieved January 21, 2010.
154. January 28, 2010 Charles Petit (January 28, 2010). "Quantum Computer Simulates Hydrogen Molecule Just Right" (https://www.wired.com/wiredscience/2010/01/quantum-computer-hydrogen-simulation/). *Wired*. Retrieved February 5, 2010.

155. February 4, 2010 Larry Hardesty. "First germanium laser brings us closer to 'optical computers' " (https://web.archive.org/web/20111224181702/http://www.physorg.com/news184493799.html). Archived from the original (http://www.physorg.com/news184493799.html) on December 24, 2011. Retrieved February 4, 2010.
156. February 6, 2010 Science Daily. "Quantum Computing Leap Forward: Altering a Lone Electron Without Disturbing Its Neighbors" (https://www.sciencedaily.com/releases/2010/02/100205162953.htm). Retrieved February 6, 2010.
157. March 18, 2010 Jason Palmer (March 17, 2010). "Team's quantum object is biggest by factor of billions" (http://news.bbc.co.uk/2/hi/sci/tech/8570836.stm). *BBC News*. Retrieved March 20, 2010.
158. University of Cambridge. "Cambridge discovery could pave the way for quantum computing" (https://go.gale.com/ps/i.do?id=GALE%7CA221455370&sid=sitemap&v=2.1&it=r&p=EAIM&sw=w&userGroupName=anon%7E3ab19270&aty=open-web-entry). Retrieved March 18, 2010.
159. April 1, 2010 ScienceDaily. "Racetrack Ion Trap Is a Contender in Quantum Computing Quest" (https://www.sciencedaily.com/releases/2010/04/100401130336.htm). Retrieved April 3, 2010.
160. April 21, 2010 Rice University (April 21, 2010). "Bizarre matter could find use in quantum computers" (https://phys.org/news/2010-04-bizarre-quantum-odd-electron-fault-tolerant.html). Retrieved August 29, 2018.
161. May 27, 2010 E. Vetsch; et al. "German physicists develop a quantum interface between light and atoms" (https://web.archive.org/web/20111219181729/http://www.physorg.com/news194169329.html). Archived from the original (http://www.physorg.com/news194169329.html) on December 19, 2011. Retrieved April 22, 2010.
162. June 3, 2010 Isabelle Dumé (June 5, 2010). "Entangling photons with electricity" (https://physicsworld.com/a/entangling-photons-with-electricity/). *Physics World*. Retrieved July 21, 2023.
163. August 29, 2010 Munro, W. J; Harrison, K. A; Stephens, A. M; Devitt, S. J; Nemoto, K (2010). "From quantum multiplexing to high-performance quantum networking". *Nature Photonics*. **4** (11): 792–796. arXiv:0910.4038 (https://arxiv.org/abs/0910.4038). Bibcode:2010NaPho...4..792M (https://ui.adsabs.harvard.edu/abs/2010NaPho...4..792M). doi:10.1038/nphoton.2010.213 (https://doi.org/10.1038%2Fnphoton.2010.213). S2CID 119243884 (https://api.semanticscholar.org/CorpusID:119243884).
164. September 17, 2010 Kurzweil accelerating intelligence. "Two-photon optical chip enables more complex quantum computing" (http://www.kurzweilai.net/two-photon-optical-chip-enables-more-complex-quantum-computing). Retrieved September 17, 2010.
165. "Toward a Useful Quantum Computer: Researchers Design and test Microfabricated Planar Ion Traps" (https://www.sciencedaily.com/releases/2010/05/100526091044.htm). *ScienceDaily*. May 28, 2010. Retrieved September 20, 2010.
166. "Quantum Future: Designing and Testing Microfabricated Planar Ion Traps" (http://www.gtri.gatech.edu/casestudy/microfabricated-planar-ion-traps). Georgia Tech Research Institute. Retrieved September 20, 2010.
167. Aaronson, Scott; Arkhipov, Alex (2011). "The Computational Complexity of Linear Optics". *Proceedings of the 43rd annual ACM symposium on Theory of computing - STOC '11*. New York, New York, USA: ACM Press. pp. 333–342. arXiv:1011.3245 (https://arxiv.org/abs/1011.3245). doi:10.1145/1993636.1993682 (https://doi.org/10.1145%2F1993636.1993682). ISBN 978-1-4503-0691-1.
168. December 23, 2010 TU Delft. "TU scientists in Nature: Better control of building blocks for quantum computer" (https://web.archive.org/web/20101224162118/http://www.tudelft.nl/live/pagina.jsp?id=2136915a-f72a-441a-8783-b0b0e91cb48f&lang=en). Archived from the original (http://www.tudelft.nl/live/pagina.jsp?id=2136915a-f72a-441a-8783-b0b0e91cb48f&lang=en) on December 24, 2010. Retrieved December 26, 2010.

169. Simmons, Stephanie; Brown, Richard M; Riemann, Helge; Abrosimov, Nikolai V; Becker, Peter; Pohl, Hans-Joachim; Thewalt, Mike L. W; Itoh, Kohei M; Morton, John J. L (2011). "Entanglement in a solid-state spin ensemble". *Nature*. **470** (7332): 69–72. arXiv:1010.0107 (https://arxiv.org/abs/1010.0107). Bibcode:2011Natur.470...69S (https://ui.adsabs.harvard.edu/abs/2011Natur.470...69S). doi:10.1038/nature09696 (https://doi.org/10.1038%2Fnature09696). PMID 21248751 (https://pubmed.ncbi.nlm.nih.gov/21248751). S2CID 4322097 (https://api.semanticscholar.org/CorpusID:4322097).
170. February 14, 2011 UC Santa Barbara Office of Public Affairs. "International Team of Scientists Says It's High 'Noon' for Microwave Photons" (http://www.ia.ucsb.edu/pa/display.aspx?pkey=2428). Retrieved February 16, 2011.
171. February 24, 2011 Kurzweil Accelerating Intelligence. " 'Quantum antennas' enable exchange of quantum information between two memory cells" (http://www.kurzweilai.net/quantum-antennas-enable-exchange-of-quantum-information-between-two-memory-cells). Retrieved February 24, 2011.
172. Peruzzo, Alberto; Laing, Anthony; Politi, Alberto; Rudolph, Terry; O'Brien, Jeremy L (2011). "Multimode quantum interference of photons in multiport integrated devices" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3072100). *Nature Communications*. **2**: 224. arXiv:1007.1372 (https://arxiv.org/abs/1007.1372). Bibcode:2011NatCo...2..224P (https://ui.adsabs.harvard.edu/abs/2011NatCo...2..224P). doi:10.1038/ncomms1228 (https://doi.org/10.1038%2Fncomms1228). PMC 3072100 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3072100). PMID 21364563 (https://pubmed.ncbi.nlm.nih.gov/21364563).
173. March 7, 2011 KFC. "New Magnetic Resonance Technique Could Revolutionise Quantum Computing" (https://www.technologyreview.com/2011/03/07/196521/new-magnetic-resonance-technique-could-revolutionise-quantum-computing/). Retrieved June 1, 2020.
174. March 17, 2011 Christof Weitenberg; Manuel Endres; Jacob F. Sherson; Marc Cheneau; Peter Schauß; Takeshi Fukuhara; Immanuel Bloch & Stefan Kuhr. "A Quantum Pen for Single Atoms" (https://web.archive.org/web/20110318143231/http://www.mpq.mpg.de/cms/mpq/en/news/press/11_03_17.html). Archived from the original (http://www.mpq.mpg.de/cms/mpq/en/news/press/11_03_17.html) on March 18, 2011. Retrieved March 19, 2011.
175. March 21, 2011 Cordisnews. "German research brings us one step closer to quantum computing" (https://web.archive.org/web/20121011161855/http://cordis.europa.eu/fetch?CALLER=EN_NEWS&ACTION=D&SESSION=&RCN=33212). Archived from the original (http://cordis.europa.eu/fetch?CALLER=EN_NEWS&ACTION=D&SESSION=&RCN=33212) on October 11, 2012. Retrieved March 22, 2011.
176. Monz, T; Schindler, P; Barreiro, J. T; Chwalla, M; Nigg, D; Coish, W. A; Harlander, M; Hänsel, W; Hennrich, M; Blatt, R (2011). "14-Qubit Entanglement: Creation and Coherence". *Physical Review Letters*. **106** (13): 130506. arXiv:1009.6126 (https://arxiv.org/abs/1009.6126). Bibcode:2011PhRvL.106m0506M (https://ui.adsabs.harvard.edu/abs/2011PhRvL.106m0506M). doi:10.1103/PhysRevLett.106.130506 (https://doi.org/10.1103%2FPhysRevLett.106.130506). PMID 21517367 (https://pubmed.ncbi.nlm.nih.gov/21517367). S2CID 8155660 (https://api.semanticscholar.org/CorpusID:8155660).
177. May 12, 2011 Physicsworld.com. "Quantum-computing firm opens the box" (https://web.archive.org/web/20110515083848/http://physicsworld.com/cws/article/news/45960). Archived from the original (http://physicsworld.com/cws/article/news/45960) on May 15, 2011. Retrieved May 17, 2011.
178. Physorg.com (May 26, 2011). "Repetitive error correction demonstrated in a quantum processor" (https://web.archive.org/web/20120107024333/http://www.physorg.com/news/2011-05-quantum-repetitive-error-processor.html). *physorg.com*. Archived from the original (http://www.physorg.com/news/2011-05-quantum-repetitive-error-processor.html) on January 7, 2012. Retrieved May 26, 2011.
179. June 27, 2011 UC Santa Barbara. "International Team Demonstrates Subatomic Quantum Memory in Diamond" (http://www.ia.ucsb.edu/pa/display.aspx?pkey=2519). Retrieved June 29, 2011.

180. July 15, 2011 Nanowerk News. "Quantum computing breakthrough in the creation of massive numbers of entangled qubits" (http://www.nanowerk.com/news/newsid=22133.php). Retrieved July 18, 2011.
181. July 20, 2011 Nanowerk News. "Scientists take the next major step toward quantum computing" (http://www.nanowerk.com/news/newsid=22174.php). Retrieved July 20, 2011.
182. August 2, 2011 nanowerk. "Dramatic simplification paves the way for building a quantum computer" (http://www.nanowerk.com/news/newsid=22292.php). Retrieved August 3, 2011.
183. Ospelkaus, C; Warring, U; Colombe, Y; Brown, K. R; Amini, J. M; Leibfried, D; Wineland, D. J (2011). "Microwave quantum logic gates for trapped ions". *Nature*. **476** (7359): 181–184. arXiv:1104.3573 (https://arxiv.org/abs/1104.3573). Bibcode:2011Natur.476..181O (https://ui.adsabs.harvard.edu/abs/2011Natur.476..181O). doi:10.1038/nature10290 (https://doi.org/10.1038%2Fnature10290). PMID 21833084 (https://pubmed.ncbi.nlm.nih.gov/21833084). S2CID 2902510 (https://api.semanticscholar.org/CorpusID:2902510).
184. August 30, 2011 Laura Ost. "NIST Achieves Record-Low Error Rate for Quantum Information Processing with One Qubit" (https://www.nist.gov/pml/div688/qubit-083011.cfm). Retrieved September 3, 2011.
185. September 1, 2011 Mariantoni, M; Wang, H; Yamamoto, T; Neeley, M; Bialczak, R. C; Chen, Y; Lenander, M; Lucero, E; O'Connell, A. D; Sank, D; Weides, M; Wenner, J; Yin, Y; Zhao, J; Korotkov, A. N; Cleland, A. N; Martinis, J. M (2011). "Implementing the Quantum von Neumann Architecture with Superconducting Circuits". *Science*. **334** (6052): 61–65. arXiv:1109.3743 (https://arxiv.org/abs/1109.3743). Bibcode:2011Sci...334...61M (https://ui.adsabs.harvard.edu/abs/2011Sci...334...61M). doi:10.1126/science.1208517 (https://doi.org/10.1126%2Fscience.1208517). PMID 21885732 (https://pubmed.ncbi.nlm.nih.gov/21885732). S2CID 11483576 (https://api.semanticscholar.org/CorpusID:11483576).
186. Jablonski, Chris (October 4, 2011). "One step closer to quantum computers" (https://www.zdnet.com/article/one-step-closer-to-quantum-computers/). *ZDnet*. Retrieved August 29, 2018.
187. December 2, 2011 Clara Moskowitz; Ian Walmsley; Michael Sprague. "Two Diamonds Linked by Strange Quantum Entanglement" (http://www.livescience.com/17264-quantum-entanglement-macroscopic-diamonds.html). Retrieved December 2, 2011.
188. Bian, Z; Chudak, F; MacReady, W. G; Clark, L; Gaitan, F (2013). "Experimental determination of Ramsey numbers with quantum annealing". *Physical Review Letters*. **111** (13): 130505. arXiv:1201.1842 (https://arxiv.org/abs/1201.1842). Bibcode:2013PhRvL.111m0505B (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111m0505B). doi:10.1103/PhysRevLett.111.130505 (https://doi.org/10.1103%2FPhysRevLett.111.130505). PMID 24116761 (https://pubmed.ncbi.nlm.nih.gov/24116761). S2CID 1303361 (https://api.semanticscholar.org/CorpusID:1303361).
189. Fuechsle, M; Miwa, J. A; Mahapatra, S; Ryu, H; Lee, S; Warschkow, O; Hollenberg, L. C; Klimeck, G; Simmons, M. Y (February 19, 2012). "A single-atom transistor". *Nature Nanotechnology*. **7** (4): 242–246. Bibcode:2012NatNa...7..242F (https://ui.adsabs.harvard.edu/abs/2012NatNa...7..242F). doi:10.1038/nnano.2012.21 (https://doi.org/10.1038%2Fnnano.2012.21). PMID 22343383 (https://pubmed.ncbi.nlm.nih.gov/22343383). S2CID 14952278 (https://api.semanticscholar.org/CorpusID:14952278).
190. John Markoff (February 19, 2012). "Physicists Create a Working Transistor From a Single Atom" (https://www.nytimes.com/2012/02/20/science/physicists-create-a-working-transistor-from-a-single-atom.html?partner=rss&emc=rss). *The New York Times*. Retrieved February 19, 2012.

191. Grotz, Bernhard; Hauf, Moritz V; Dankerl, Markus; Naydenov, Boris; Pezzagna, Sébastien; Meijer, Jan; Jelezko, Fedor; Wrachtrup, Jörg; Stutzmann, Martin; Reinhard, Friedemann; Garrido, Jose A (2012). "Charge state manipulation of qubits in diamond" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3316888). *Nature Communications*. **3**: 729. Bibcode:2012NatCo...3..729G (https://ui.adsabs.harvard.edu/abs/2012NatCo...3..729G). doi:10.1038/ncomms1729 (https://doi.org/10.1038%2Fncomms1729). PMC 3316888 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3316888). PMID 22395620 (https://pubmed.ncbi.nlm.nih.gov/22395620).
192. Britton, J. W; Sawyer, B. C; Keith, A. C; Wang, C. C; Freericks, J. K; Uys, H; Biercuk, M. J; Bollinger, J. J (April 26, 2012). "Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins". *Nature*. **484** (7395): 489–492. arXiv:1204.5789 (https://arxiv.org/abs/1204.5789). Bibcode:2012Natur.484..489B (https://ui.adsabs.harvard.edu/abs/2012Natur.484..489B). doi:10.1038/nature10981 (https://doi.org/10.1038%2Fnature10981). PMID 22538611 (https://pubmed.ncbi.nlm.nih.gov/22538611). S2CID 4370334 (https://api.semanticscholar.org/CorpusID:4370334).
193. Lucy Sherriff. "300 atom quantum simulator smashes qubit record" (https://www.zdnet.com/article/300-atom-quantum-simulator-smashes-qubit-record/). Retrieved February 9, 2015.
194. Yao, Xing-Can; Wang, Tian-Xiong; Chen, Hao-Ze; Gao, Wei-Bo; Fowler, Austin G; Raussendorf, Robert; Chen, Zeng-Bing; Liu, Nai-Le; Lu, Chao-Yang; Deng, You-Jin; Chen, Yu-Ao; Pan, Jian-Wei (2012). "Experimental demonstration of topological error correction". *Nature*. **482** (7386): 489–494. arXiv:0905.1542 (https://arxiv.org/abs/0905.1542). Bibcode:2012Natur.482..489Y (https://ui.adsabs.harvard.edu/abs/2012Natur.482..489Y). doi:10.1038/nature10770 (https://doi.org/10.1038%2Fnature10770). PMID 22358838 (https://pubmed.ncbi.nlm.nih.gov/22358838). S2CID 4307662 (https://api.semanticscholar.org/CorpusID:4307662).
195. 1QBit. "1QBit Website" (http://www.1qbit.com/).
196. October 14, 2012 Munro, W. J; Stephens, A. M; Devitt, S. J; Harrison, K. A; Nemoto, K (2012). "Quantum communication without the necessity of quantum memories". *Nature Photonics*. **6** (11): 777–781. arXiv:1306.4137 (https://arxiv.org/abs/1306.4137). Bibcode:2012NaPho...6..777M (https://ui.adsabs.harvard.edu/abs/2012NaPho...6..777M). doi:10.1038/nphoton.2012.243 (https://doi.org/10.1038%2Fnphoton.2012.243). S2CID 5056130 (https://api.semanticscholar.org/CorpusID:5056130).
197. Maurer, P. C; Kucsko, G; Latta, C; Jiang, L; Yao, N. Y; Bennett, S. D; Pastawski, F; Hunger, D; Chisholm, N; Markham, M; Twitchen, D. J; Cirac, J. I; Lukin, M. D (June 8, 2012). "Room-Temperature Quantum Bit Memory Exceeding One Second" (http://nrs.harvard.edu/urn-3:HUL.InstRepos:12132060). *Science* (Submitted manuscript). **336** (6086): 1283–1286. Bibcode:2012Sci...336.1283M (https://ui.adsabs.harvard.edu/abs/2012Sci...336.1283M). doi:10.1126/science.1220513 (https://doi.org/10.1126%2Fscience.1220513). PMID 22679092 (https://pubmed.ncbi.nlm.nih.gov/22679092). S2CID 2684102 (https://api.semanticscholar.org/CorpusID:2684102).
198. Peckham, Matt (July 6, 2012). "Quantum Computing at Room Temperature - Now a Reality" (http://techland.time.com/2012/07/06/quantum-computing-at-room-temperature-now-a-reality/). *Magazine/Periodical*. Time Magazine (Techland) Time Inc. p. 1. Retrieved August 5, 2012.
199. Koh, Dax Enshan; Hall, Michael J. W; Setiawan; Pope, James E; Marletto, Chiara; Kay, Alastair; Scarani, Valerio; Ekert, Artur (2012). "Effects of Reduced Measurement Independence on Bell-Based Randomness Expansion". *Physical Review Letters*. **109** (16): 160404. arXiv:1202.3571 (https://arxiv.org/abs/1202.3571). Bibcode:2012PhRvL.109p0404K (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109p0404K). doi:10.1103/PhysRevLett.109.160404 (https://doi.org/10.1103%2FPhysRevLett.109.160404). PMID 23350071 (https://pubmed.ncbi.nlm.nih.gov/23350071). S2CID 18935137 (https://api.semanticscholar.org/CorpusID:18935137).

200. December 7, 2012 Horsman, C; Fowler, A. G; Devitt, S. J; Van Meter, R (2012). "Surface code quantum computing by lattice surgery". *New J. Phys*. **14** (12): 123011. arXiv:1111.4022 (https://arxiv.org/abs/1111.4022). Bibcode:2012NJPh...14l3011H (https://ui.adsabs.harvard.edu/abs/2012NJPh...14l3011H). doi:10.1088/1367-2630/14/12/123011 (https://doi.org/10.1088%2F1367-2630%2F14%2F12%2F123011). S2CID 119212756 (https://api.semanticscholar.org/CorpusID:119212756).
201. Kastrenakes, Jacob (November 14, 2013). "Researchers smash through quantum computer storage record" (https://www.theverge.com/2013/11/14/5104668/qubits-stored-for-39-minutes-quantum-computer-new-record). *Webzine*. The Verge. Retrieved November 20, 2013.
202. "Quantum Computer Breakthrough 2013" (https://web.archive.org/web/20181002141518/http://welldonestuff.com/quantum-computer-breakthrough-2013/). November 24, 2013. Archived from the original (http://welldonestuff.com/quantum-computer-breakthrough-2013/) on October 2, 2018. Retrieved October 2, 2018.
203. October 10, 2013 Devitt, S. J; Stephens, A. M; Munro, W. J; Nemoto, K (2013). "Requirements for fault-tolerant factoring on an atom-optics quantum computer". *Nature Communications*. **4**: 2524. arXiv:1212.4934 (https://arxiv.org/abs/1212.4934). Bibcode:2013NatCo...4.2524D (https://ui.adsabs.harvard.edu/abs/2013NatCo...4.2524D). doi:10.1038/ncomms3524 (https://doi.org/10.1038%2Fncomms3524). PMID 24088785 (https://pubmed.ncbi.nlm.nih.gov/24088785). S2CID 7229103 (https://api.semanticscholar.org/CorpusID:7229103).
204. "Penetrating Hard Targets project" (https://web.archive.org/web/20170830105417/https://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/). Archived from the original (https://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/) on August 30, 2017. Retrieved September 16, 2017.
205. "NSA seeks to develop quantum computer to crack nearly every kind of encryption « Kurzweil" (https://www.kurzweilai.net/nsa-seeks-to-develop-quantum-computer-to-crack-nearly-every-kind-of-encryption).
206. NSA seeks to build quantum computer that could crack most types of encryption – Washington Post (https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html)
207. Dockterman, Eliana (January 2, 2014). "The NSA Is Building a Computer to Crack Almost Any Code" (https://nation.time.com/2014/01/02/the-nsa-is-building-a-computer-to-crack-almost-any-code/). *Time* – via nation.time.com.
208. August 4, 2014 Nemoto, K.; Trupke, M.; Devitt, S. J; Stephens, A. M; Scharfenberger, B; Buczak, K; Nobauer, T; Everitt, M. S; Schmiedmayer, J; Munro, W. J (2014). "Photonic architecture for scalable quantum information processing in diamond". *Physical Review X*. **4** (3): 031022. arXiv:1309.4277 (https://arxiv.org/abs/1309.4277). Bibcode:2014PhRvX...4c1022N (https://ui.adsabs.harvard.edu/abs/2014PhRvX...4c1022N). doi:10.1103/PhysRevX.4.031022 (https://doi.org/10.1103%2FPhysRevX.4.031022). S2CID 118418371 (https://api.semanticscholar.org/CorpusID:118418371).
209. Nigg, D; Müller, M; Martinez, M. A; Schindler, P; Hennrich, M; Monz, T; Martin-Delgado, M. A; Blatt, R (July 18, 2014). "Quantum computations on a topologically encoded qubit". *Science*. **345** (6194): 302–305. arXiv:1403.5426 (https://arxiv.org/abs/1403.5426). Bibcode:2014Sci...345..302N (https://ui.adsabs.harvard.edu/abs/2014Sci...345..302N). doi:10.1126/science.1253742 (https://doi.org/10.1126%2Fscience.1253742). PMID 24925911 (https://pubmed.ncbi.nlm.nih.gov/24925911). S2CID 9677048 (https://api.semanticscholar.org/CorpusID:9677048).
210. Markoff, John (May 29, 2014). "Scientists Report Finding Reliable Way to Teleport Data" (https://www.nytimes.com/2014/05/30/science/scientists-report-finding-reliable-way-to-teleport-data.html). *The New York Times*. Retrieved May 29, 2014.

211. Pfaff, W; Hensen, B. J; Bernien, H; Van Dam, S. B; Blok, M. S; Taminiau, T. H; Tiggelman, M. J; Schouten, R. N; Markham, M; Twitchen, D. J; Hanson, R (May 29, 2014). "Unconditional quantum teleportation between distant solid-state quantum bits". *Science*. **345** (6196): 532–535. arXiv:1404.4369 (https://arxiv.org/abs/1404.4369). Bibcode:2014Sci...345..532P (https://ui.adsabs.harvard.edu/abs/2014Sci...345..532P). doi:10.1126/science.1253512 (https://doi.org/10.1126%2Fscience.1253512). PMID 25082696 (https://pubmed.ncbi.nlm.nih.gov/25082696). S2CID 2190249 (https://api.semanticscholar.org/CorpusID:2190249).
212. Zhong, Manjin; Hedges, Morgan P; Ahlefeldt, Rose L; Bartholomew, John G; Beavan, Sarah E; Wittig, Sven M; Longdell, Jevon J; Sellars, Matthew J (2015). "Optically addressable nuclear spins in a solid with a six-hour coherence time". *Nature*. **517** (7533): 177–180. Bibcode:2015Natur.517..177Z (https://ui.adsabs.harvard.edu/abs/2015Natur.517..177Z). doi:10.1038/nature14025 (https://doi.org/10.1038%2Fnature14025). PMID 25567283 (https://pubmed.ncbi.nlm.nih.gov/25567283). S2CID 205241727 (https://api.semanticscholar.org/CorpusID:205241727).
213. April 13, 2015 "Breakthrough opens door to affordable quantum computers" (http://newsroom.unsw.edu.au/news/science-tech/breakthrough-opens-door-affordable-quantum-computers). Retrieved April 16, 2015.
214. Córcoles, A.D; Magesan, Easwar; Srinivasan, Srikanth J; Cross, Andrew W; Steffen, M; Gambetta, Jay M; Chow, Jerry M (2015). "Demonstration of a quantum error detection code using a square lattice of four superconducting qubits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4421819). *Nature Communications*. **6**: 6979. arXiv:1410.6419 (https://arxiv.org/abs/1410.6419). Bibcode:2015NatCo...6.6979C (https://ui.adsabs.harvard.edu/abs/2015NatCo...6.6979C). doi:10.1038/ncomms7979 (https://doi.org/10.1038%2Fncomms7979). PMC 4421819 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4421819). PMID 25923200 (https://pubmed.ncbi.nlm.nih.gov/25923200).
215. June 22, 2015 "D-Wave Systems Inc., the world's first quantum computing company, today announced that it has broken the 1000 qubit barrier" (https://web.archive.org/web/20180115184711/https://www.dwavesys.com/press-releases/d-wave-systems-breaks-1000-qubit-quantum-computing-barrier). Archived from the original (http://www.dwavesys.com/press-releases/d-wave-systems-breaks-1000-qubit-quantum-computing-barrier) on January 15, 2018. Retrieved June 22, 2015.
216. October 6, 2015 "Crucial hurdle overcome in quantum computing" (http://www.newsroom.unsw.edu.au/news/science-tech/crucial-hurdle-overcome-quantum-computing). Retrieved October 6, 2015.
217. Monz, T; Nigg, D; Martinez, E. A; Brandl, M. F; Schindler, P; Rines, R; Wang, S. X; Chuang, I. L; Blatt, R; et al. (March 4, 2016). "Realization of a scalable Shor algorithm". *Science*. **351** (6277): 1068–1070. arXiv:1507.08852 (https://arxiv.org/abs/1507.08852). Bibcode:2016Sci...351.1068M (https://ui.adsabs.harvard.edu/abs/2016Sci...351.1068M). doi:10.1126/science.aad9480 (https://doi.org/10.1126%2Fscience.aad9480). PMID 26941315 (https://pubmed.ncbi.nlm.nih.gov/26941315). S2CID 17426142 (https://api.semanticscholar.org/CorpusID:17426142).
218. September 29, 2016 Devitt, S. J (2016). "Performing quantum computing experiments in the cloud". *Physical Review A*. **94** (3): 032329. arXiv:1605.05709 (https://arxiv.org/abs/1605.05709). Bibcode:2016PhRvA..94c2329D (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94c2329D). doi:10.1103/PhysRevA.94.032329 (https://doi.org/10.1103%2FPhysRevA.94.032329). S2CID 119217150 (https://api.semanticscholar.org/CorpusID:119217150).
219. Alsina, D; Latorre, J. I (2016). "Experimental test of Mermin inequalities on a five-qubit quantum computer". *Physical Review A*. **94** (1): 012314. arXiv:1605.04220 (https://arxiv.org/abs/1605.04220). Bibcode:2016PhRvA..94a2314A (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94a2314A). doi:10.1103/PhysRevA.94.012314 (https://doi.org/10.1103%2FPhysRevA.94.012314). S2CID 119189277 (https://api.semanticscholar.org/CorpusID:119189277).

220. o'Malley, P. J. J; Babbush, R; Kivlichan, I. D; Romero, J; McClean, J. R; Barends, R; Kelly, J; Roushan, P; Tranter, A; Ding, N; Campbell, B; Chen, Y; Chen, Z; Chiaro, B; Dunsworth, A; Fowler, A. G; Jeffrey, E; Lucero, E; Megrant, A; Mutus, J. Y; Neeley, M; Neill, C; Quintana, C; Sank, D; Vainsencher, A; Wenner, J; White, T. C; Coveney, P. V; Love, P. J; Neven, H; et al. (July 18, 2016). "Scalable Quantum Simulation of Molecular Energies". *Physical Review X*. **6** (3): 031007. arXiv:1512.06860 (https://arxiv.org/abs/1512.06860). Bibcode:2016PhRvX...6c1007O (https://ui.adsabs.harvard.edu/abs/2016PhRvX...6c1007O). doi:10.1103/PhysRevX.6.031007 (https://doi.org/10.1103%2FPhysRevX.6.031007). S2CID 4884151 (https://api.semanticscholar.org/CorpusID:4884151).
221. November 2, 2016 Devitt, S. J; Greentree, A. D; Stephens, A. M; Van Meter, R (2016). "High-speed quantum networking by ship" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5090252). *Scientific Reports*. **6**: 36163. arXiv:1605.05709 (https://arxiv.org/abs/1605.05709). Bibcode:2016NatSR...636163D (https://ui.adsabs.harvard.edu/abs/2016NatSR...636163D). doi:10.1038/srep36163 (https://doi.org/10.1038%2Fsrep36163). PMC 5090252 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5090252). PMID 27805001 (https://pubmed.ncbi.nlm.nih.gov/27805001).
222. "D-Wave Announces D-Wave 2000Q Quantum Computer and First System Order | D-Wave Systems" (https://web.archive.org/web/20170127044404/http://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order). *www.dwavesys.com*. Archived from the original (http://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order) on January 27, 2017. Retrieved January 26, 2017.
223. Lekitsch, B; Weidt, S; Fowler, A. G; Mølmer, K; Devitt, S. J; Wunderlich, C; Hensinger, W. K (February 1, 2017). "Blueprint for a microwave trapped ion quantum computer" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5287699). *Science Advances*. **3** (2): e1601540. arXiv:1508.00420 (https://arxiv.org/abs/1508.00420). Bibcode:2017SciA....3E1540L (https://ui.adsabs.harvard.edu/abs/2017SciA....3E1540L). doi:10.1126/sciadv.1601540 (https://doi.org/10.1126%2Fsciadv.1601540). PMC 5287699 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5287699). PMID 28164154 (https://pubmed.ncbi.nlm.nih.gov/28164154).
224. Meredith Rutland Bauer (May 17, 2017). "IBM Just Made a 17 Qubit Quantum Processor, Its Most Powerful One Yet" (https://motherboard.vice.com/en_us/article/wnwk5w/ibm-17-qubit-quantum-processor-computer-google). *Motherboard*.
225. "Qudits: The Real Future of Quantum Computing?" (https://spectrum.ieee.org/qudits-the-real-future-of-quantum-computing). *IEEE Spectrum*. June 28, 2017. Retrieved June 29, 2017.
226. "Microsoft makes play for next wave of computing with quantum computing toolkit" (https://arstechnica.com/gadgets/2017/09/microsoft-quantum-toolkit/). *arstechnica.com*. September 25, 2017. Retrieved October 5, 2017.
227. "IBM Raises the Bar with a 50-Qubit Quantum Computer" (https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/). *MIT Technology Review*. Retrieved December 13, 2017.
228. Ren, Ji-Gang; Xu, Ping; Yong, Hai-Lin; Zhang, Liang; Liao, Sheng-Kai; Yin, Juan; Liu, Wei-Yue; Cai, Wen-Qi; Yang, Meng; Li, Li; Yang, Kui-Xing (August 9, 2017). "Ground-to-satellite quantum teleportation" (https://www.nature.com/articles/nature23675/). *Nature*. **549** (7670): 70–73. arXiv:1707.00934 (https://arxiv.org/abs/1707.00934). Bibcode:2017Natur.549...70R (https://ui.adsabs.harvard.edu/abs/2017Natur.549...70R). doi:10.1038/nature23675 (https://doi.org/10.1038%2Fnature23675). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 28825708 (https://pubmed.ncbi.nlm.nih.gov/28825708). S2CID 4468803 (https://api.semanticscholar.org/CorpusID:4468803).
229. Preskill, John (August 6, 2018). "Quantum Computing in the NISQ era and beyond" (https://quantum-journal.org/papers/q-2018-08-06-79/). *Quantum*. **2**: 79. arXiv:1801.00862 (https://arxiv.org/abs/1801.00862). Bibcode:2018Quant...2...79P (https://ui.adsabs.harvard.edu/abs/2018Quant...2...79P). doi:10.22331/q-2018-08-06-79 (https://doi.org/10.22331%2Fq-2018-08-06-79). ISSN 2521-327X (https://search.worldcat.org/issn/2521-327X).

230. Hignett, Katherine (February 16, 2018). "Physics Creates New Form Of Light That Could Drive The Quantum Computing Revolution" (http://www.newsweek.com/photons-light-physics-808862). *Newsweek*. Retrieved February 17, 2018.
231. Liang, Q. Y; Venkatramani, A. V; Cantu, S. H; Nicholson, T. L; Gullans, M. J; Gorshkov, A. V; Thompson, J. D; Chin, C; Lukin, M. D; Vuletić, V (February 16, 2018). "Observation of three-photon bound states in a quantum nonlinear medium" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6467536). *Science*. **359** (6377): 783–786. arXiv:1709.01478 (https://arxiv.org/abs/1709.01478). Bibcode:2018Sci...359..783L (https://ui.adsabs.harvard.edu/abs/2018Sci...359..783L). doi:10.1126/science.aao7293 (https://doi.org/10.1126%2Fscience.aao7293). PMC 6467536 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6467536). PMID 29449489 (https://pubmed.ncbi.nlm.nih.gov/29449489).
232. "Scientists make major quantum computing breakthrough" (https://www.independent.co.uk/life-style/gadgets-and-tech/news/quantum-computing-logic-gates-oxford-university-breakthrough-latest-discovery-a8235281.html). *Independent.co.uk*. March 2018. Archived (https://ghostarchive.org/archive/20220507/https://www.independent.co.uk/life-style/gadgets-and-tech/news/quantum-computing-logic-gates-oxford-university-breakthrough-latest-discovery-a8235281.html) from the original on May 7, 2022.
233. Giles, Martin (February 15, 2018). "Old-fashioned silicon might be the key to building ubiquitous quantum computers" (https://www.technologyreview.com/s/610273/old-fashioned-silicon-might-be-the-key-to-building-ubiquitous-quantum-computers/). *MIT Technology Review*. Retrieved July 5, 2018.
234. Emily Conover (March 5, 2018). "Google moves toward quantum supremacy with 72-qubit computer" (https://www.sciencenews.org/article/google-moves-toward-quantum-supremacy-72-qubit-computer). *Science News*. Retrieved August 28, 2018.
235. Forrest, Conner (June 12, 2018). "Why Intel's smallest spin qubit chip could be a turning point in quantum computing" (https://www.techrepublic.com/article/why-intels-smallest-spin-qubit-chip-could-be-a-turning-point-in-quantum-computing/). *TechRepublic*. Retrieved July 12, 2018.
236. Hsu, Jeremy (January 9, 2018). "CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy" (https://spectrum.ieee.org/intels-49qubit-chip-aims-for-quantum-supremacy). Institute of Electrical and Electronics Engineers. Retrieved July 5, 2018.
237. Nagata, K; Kuramitani, K; Sekiguchi, Y; Kosaka, H (August 13, 2018). "Universal holonomic quantum gates over geometric spin qubits with polarised microwaves" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6089953). *Nature Communications*. **9** (3227): 3227. Bibcode:2018NatCo...9.3227N (https://ui.adsabs.harvard.edu/abs/2018NatCo...9.3227N). doi:10.1038/s41467-018-05664-w (https://doi.org/10.1038%2Fs41467-018-05664-w). PMC 6089953 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6089953). PMID 30104616 (https://pubmed.ncbi.nlm.nih.gov/30104616).
238. Lenzini, Francesco (December 7, 2018). "Integrated photonic platform for quantum information with continuous variables" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6286167). *Science Advances*. **4** (12): eaat9331. arXiv:1804.07435 (https://arxiv.org/abs/1804.07435). Bibcode:2018SciA....4.9331L (https://ui.adsabs.harvard.edu/abs/2018SciA....4.9331L). doi:10.1126/sciadv.aat9331 (https://doi.org/10.1126%2Fsciadv.aat9331). PMC 6286167 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6286167). PMID 30539143 (https://pubmed.ncbi.nlm.nih.gov/30539143).
239. "Ion-based commercial quantum computer is a first" (https://physicsworld.com/a/ion-based-commercial-quantum-computer-is-a-first/). *Physics World*. December 17, 2018.
240. "IonQ" (https://ionq.com/).
241. 115th Congress (2018) (June 26, 2018). "H.R. 6227 (115th)" (https://www.govtrack.us/congress/bills/115/hr6227). *Legislation*. GovTrack.us. Retrieved February 11, 2019. "National Quantum Initiative Act"

242. "President Trump has signed a $1.2 billon law to boost US quantum tech" (https://www.technologyreview.com/the-download/612679/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/). *MIT Technology Review*. Retrieved February 11, 2019.
243. "US National Quantum Initiative Act passed unanimously" (https://thestack.com/data-centre/2018/12/18/us-national-quantum-initiative-act/). *The Stack*. December 18, 2018. Retrieved February 11, 2019.
244. Aron, Jacob (January 8, 2019). "IBM unveils its first commercial quantum computer" (https://www.newscientist.com/article/2189909-ibm-unveils-its-first-commercial-quantum-computer/). *New Scientist*. Retrieved January 8, 2019.
245. "IBM unveils its first commercial quantum computer" (https://techcrunch.com/2019/01/08/ibm-unveils-its-first-commercial-quantum-computer/). *TechCrunch*. January 8, 2019. Retrieved February 18, 2019.
246. Kokail, C; Maier, C; Van Bijnen, R; Brydges, T; Joshi, M. K; Jurcevic, P; Muschik, C. A; Silvi, P; Blatt, R; Roos, C; Zoller, P (May 15, 2019). "Self-verifying variational quantum simulation of lattice models". *Science*. **569** (7756): 355–360. arXiv:1810.03421 (https://arxiv.org/abs/1810.03421). Bibcode:2019Natur.569..355K (https://ui.adsabs.harvard.edu/abs/2019Natur.569..355K). doi:10.1038/s41586-019-1177-4 (https://doi.org/10.1038%2Fs41586-019-1177-4). PMID 31092942 (https://pubmed.ncbi.nlm.nih.gov/31092942). S2CID 53595106 (https://api.semanticscholar.org/CorpusID:53595106).
247. UNSW Media (May 23, 2019). "'Noise-cancelling headphones' for quantum computers: international collaboration launched" (https://newsroom.unsw.edu.au/news/science-tech/noise-cancelling-headphones%E2%80%99-quantum-computers-international-collaboration#:~:text=A%20new%20project%20to%20develop,quantum%20building%20blocks%2C%20or%20qubits.&text=Morello%27s%20team%20was%20the%20first,information%20in%20a%20silicon%20chip). *UNSW Newsroom*. University of New South Wales. Retrieved April 16, 2022.
248. "Cancelling quantum noise" (https://www.uts.edu.au/about/faculty-engineering-and-information-technology/news/cancelling-quantum-noise). May 23, 2019.
249. Unden, T.; Louzon, D.; Zwolak, M.; Zurek, W. H.; Jelezko, F. (October 1, 2019). "Revealing the Emergence of Classicality Using Nitrogen-Vacancy Centers" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7003699). *Physical Review Letters*. **123** (140402): 140402. arXiv:1809.10456 (https://arxiv.org/abs/1809.10456). Bibcode:2019PhRvL.123n0402U (https://ui.adsabs.harvard.edu/abs/2019PhRvL.123n0402U). doi:10.1103/PhysRevLett.123.140402 (https://doi.org/10.1103%2FPhysRevLett.123.140402). PMC 7003699 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7003699). PMID 31702205 (https://pubmed.ncbi.nlm.nih.gov/31702205).
250. Cho, A. (September 13, 2019). "Quantum Darwinism seen in diamond traps". *Science*. **365** (6458): 1070. Bibcode:2019Sci...365.1070C (https://ui.adsabs.harvard.edu/abs/2019Sci...365.1070C). doi:10.1126/science.365.6458.1070 (https://doi.org/10.1126%2Fscience.365.6458.1070). PMID 31515367 (https://pubmed.ncbi.nlm.nih.gov/31515367). S2CID 202567042 (https://api.semanticscholar.org/CorpusID:202567042).
251. "Google may have taken a step towards quantum computing 'supremacy' (updated)" (https://www.engadget.com/2019/09/23/google-quantum-supremacy/). *Engadget*. September 23, 2019. Retrieved September 24, 2019.
252. Porter, Jon (September 23, 2019). "Google may have just ushered in an era of 'quantum supremacy'" (https://www.theverge.com/2019/9/23/20879485/google-quantum-supremacy-qubits-nasa). *The Verge*. Retrieved September 24, 2019.
253. Murgia, Waters, Madhumita, Richard (September 20, 2019). "Google claims to have reached quantum supremacy" (https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17). *Financial Times*. Archived (https://ghostarchive.org/archive/20221210/https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17) from the original on December 10, 2022. Retrieved September 24, 2019.

254. "Google Builds Circuit to Solve One of Quantum Computing's Biggest Problems - IEEE Spectrum" (https://spectrum.ieee.org/google-team-builds-circuit-to-solve-one-of-quantum-computings-biggest-problems).
255. Garisto, Daniel. "Quantum Computer Made from Photons Achieves a New Record" (https://www.scientificamerican.com/article/quantum-computer-made-from-photons-achieves-a-new-record/). *Scientific American*. Retrieved June 30, 2021.
256. "Hot qubits made in Sydney break one of the biggest constraints to practical quantum computers" (https://newsroom.unsw.edu.au/news/science-tech/hot-qubits-made-sydney-break-one-biggest-constraints-practical-quantum-computers). April 16, 2020.
257. "Engineers crack 58-year-old puzzle on way to quantum breakthrough" (https://newsroom.unsw.edu.au/news/science-tech/engineers-crack-58-year-old-puzzle-way-quantum-breakthrough). March 12, 2020.
258. "Wiring the quantum computer of the future: A novel simple build with existing technology" (https://eurekalert.org/pub_releases/2020-04/tuos-wtq042320.php).
259. "Quantum researchers able to split one photon into three" (https://phys.org/news/2020-02-quantum-photon.html). *phys.org*. Retrieved March 9, 2020.
260. Chang, C. W. Sandbo; Sabín, Carlos; Forn-Díaz, P.; Quijandría, Fernando; Vadiraj, A. M.; Nsanzineza, I.; Johansson, G.; Wilson, C. M. (January 16, 2020). "Observation of Three-Photon Spontaneous Parametric Down-Conversion in a Superconducting Parametric Cavity" (https://doi.org/10.1103%2FPhysRevX.10.011011). *Physical Review X*. **10** (1): 011011. arXiv:1907.08692 (https://arxiv.org/abs/1907.08692). Bibcode:2020PhRvX..10a1011C (https://ui.adsabs.harvard.edu/abs/2020PhRvX..10a1011C). doi:10.1103/PhysRevX.10.011011 (https://doi.org/10.1103%2FPhysRevX.10.011011).
261. "Artificial atoms create stable qubits for quantum computing" (https://phys.org/news/2020-02-artificial-atoms-stable-qubits-quantum.html). *phys.org*. Retrieved March 9, 2020.
262. Leon, R. C. C.; Yang, C. H.; Hwang, J. C. C.; Lemyre, J. Camirand; Tanttu, T.; Huang, W.; Chan, K. W.; Tan, K. Y.; Hudson, F. E.; Itoh, K. M.; Morello, A.; Laucht, A.; Pioro-Ladrière, M.; Saraiva, A.; Dzurak, A. S. (February 11, 2020). "Coherent spin control of s-, p-, d- and f-electrons in a silicon quantum dot" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7012832). *Nature Communications*. **11** (1): 797. arXiv:1902.01550 (https://arxiv.org/abs/1902.01550). Bibcode:2020NatCo..11..797L (https://ui.adsabs.harvard.edu/abs/2020NatCo..11..797L). doi:10.1038/s41467-019-14053-w (https://doi.org/10.1038%2Fs41467-019-14053-w). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 7012832 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7012832). PMID 32047151 (https://pubmed.ncbi.nlm.nih.gov/32047151).
263. "Producing single photons from a stream of single electrons" (https://phys.org/news/2020-02-photons-stream-electrons.html). *phys.org*. Retrieved March 8, 2020.
264. Hsiao, Tzu-Kan; Rubino, Antonio; Chung, Yousun; Son, Seok-Kyun; Hou, Hangtian; Pedrós, Jorge; Nasir, Ateeq; Éthier-Majcher, Gabriel; Stanley, Megan J.; Phillips, Richard T.; Mitchell, Thomas A.; Griffiths, Jonathan P.; Farrer, Ian; Ritchie, David A.; Ford, Christopher J. B. (February 14, 2020). "Single-photon emission from single-electron transport in a SAW-driven lateral light-emitting diode" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7021712). *Nature Communications*. **11** (1): 917. arXiv:1901.03464 (https://arxiv.org/abs/1901.03464). Bibcode:2020NatCo..11..917H (https://ui.adsabs.harvard.edu/abs/2020NatCo..11..917H). doi:10.1038/s41467-020-14560-1 (https://doi.org/10.1038%2Fs41467-020-14560-1). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 7021712 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7021712). PMID 32060278 (https://pubmed.ncbi.nlm.nih.gov/32060278).
265. "Scientists 'film' a quantum measurement" (https://phys.org/news/2020-02-scientists-quantum.html). *phys.org*. Retrieved March 9, 2020.

266. Pokorny, Fabian; Zhang, Chi; Higgins, Gerard; Cabello, Adán; Kleinmann, Matthias; Hennrich, Markus (February 25, 2020). "Tracking the Dynamics of an Ideal Quantum Measurement". *Physical Review Letters*. **124** (8): 080401. arXiv:1903.10398 (https://arxiv.org/abs/1903.10398). Bibcode:2020PhRvL.124h0401P (https://ui.adsabs.harvard.edu/abs/2020PhRvL.124h0401P). doi:10.1103/PhysRevLett.124.080401 (https://doi.org/10.1103%2FPhysRevLett.124.080401). PMID 32167322 (https://pubmed.ncbi.nlm.nih.gov/32167322). S2CID 85501331 (https://api.semanticscholar.org/CorpusID:85501331).
267. "Scientists measure electron spin qubit without demolishing it" (https://phys.org/news/2020-03-scientists-electron-qubit-demolishing.html). *phys.org*. Retrieved April 5, 2020.
268. Yoneda, J.; Takeda, K.; Noiri, A.; Nakajima, T.; Li, S.; Kamioka, J.; Kodera, T.; Tarucha, S. (March 2, 2020). "Quantum non-demolition readout of an electron spin in silicon" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7052195). *Nature Communications*. **11** (1): 1144. arXiv:1910.11963 (https://arxiv.org/abs/1910.11963). Bibcode:2020NatCo..11.1144Y (https://ui.adsabs.harvard.edu/abs/2020NatCo..11.1144Y). doi:10.1038/s41467-020-14818-8 (https://doi.org/10.1038%2Fs41467-020-14818-8). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 7052195 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7052195). PMID 32123167 (https://pubmed.ncbi.nlm.nih.gov/32123167).
269. "Engineers crack 58-year-old puzzle on way to quantum breakthrough" (https://phys.org/news/2020-03-year-old-puzzle-quantum-breakthrough.html). *phys.org*. Retrieved April 5, 2020.
270. Asaad, Serwan; Mourik, Vincent; Joecker, Benjamin; Johnson, Mark A. I.; Baczewski, Andrew D.; Firgau, Hannes R.; Mądzik, Mateusz T.; Schmitt, Vivien; Pla, Jarryd J.; Hudson, Fay E.; Itoh, Kohei M.; McCallum, Jeffrey C.; Dzurak, Andrew S.; Laucht, Arne; Morello, Andrea (March 2020). "Coherent electrical control of a single high-spin nucleus in silicon". *Nature*. **579** (7798): 205–209. arXiv:1906.01086 (https://arxiv.org/abs/1906.01086). Bibcode:2020Natur.579..205A (https://ui.adsabs.harvard.edu/abs/2020Natur.579..205A). doi:10.1038/s41586-020-2057-7 (https://doi.org/10.1038%2Fs41586-020-2057-7). PMID 32161384 (https://pubmed.ncbi.nlm.nih.gov/32161384). S2CID 174797899 (https://api.semanticscholar.org/CorpusID:174797899).
271. Laboratory, The Army Research. "Scientists create quantum sensor that covers entire radio frequency spectrum" (https://phys.org/news/2020-03-scientists-quantum-sensor-entire-radio.html). *phys.org*. Retrieved April 14, 2024.
272. Meyer, David H; Castillo, Zachary A; Cox, Kevin C; Kunz, Paul D (January 10, 2020). "Assessment of Rydberg atoms for wideband electric field sensing". *Journal of Physics B: Atomic, Molecular and Optical Physics*. **53** (3): 034001. arXiv:1910.00646 (https://arxiv.org/abs/1910.00646). Bibcode:2020JPhB...53c4001M (https://ui.adsabs.harvard.edu/abs/2020JPhB...53c4001M). doi:10.1088/1361-6455/ab6051 (https://doi.org/10.1088%2F1361-6455%2Fab6051). ISSN 0953-4075 (https://search.worldcat.org/issn/0953-4075). S2CID 203626886 (https://api.semanticscholar.org/CorpusID:203626886).
273. "Researchers demonstrate the missing link for a quantum internet" (https://phys.org/news/2020-03-link-quantum-internet.html). *phys.org*. Retrieved April 7, 2020.
274. Bhaskar, M. K.; Riedinger, R.; Machielse, B.; Levonian, D. S.; Nguyen, C. T.; Knall, E. N.; Park, H.; Englund, D.; Lončar, M.; Sukachev, D. D.; Lukin, M. D. (April 2020). "Experimental demonstration of memory-enhanced quantum communication". *Nature*. **580** (7801): 60–64. arXiv:1909.01323 (https://arxiv.org/abs/1909.01323). Bibcode:2020Natur.580...60B (https://ui.adsabs.harvard.edu/abs/2020Natur.580...60B). doi:10.1038/s41586-020-2103-5 (https://doi.org/10.1038%2Fs41586-020-2103-5). PMID 32238931 (https://pubmed.ncbi.nlm.nih.gov/32238931). S2CID 202539813 (https://api.semanticscholar.org/CorpusID:202539813).
275. Delbert, Caroline (April 17, 2020). "Hot Qubits Could Deliver a Quantum Computing Breakthrough" (https://www.popularmechanics.com/science/a32170397/hot-qubits-quantum-computing-breakthrough/). *Popular Mechanics*. Retrieved May 16, 2020.
276. " 'Hot' qubits crack quantum computing temperature barrier – ABC News" (https://www.abc.net.au/news/science/2020-04-16/hot-qubits-crack-quantum-computing-temperature-barrier/12132400). *www.abc.net.au*. April 15, 2020. Retrieved May 16, 2020.

277. "Hot qubits break one of the biggest constraints to practical quantum computers" (https://phys.org/news/2020-04-hot-qubits-biggest-constraints-quantum.html). *phys.org*. Retrieved May 16, 2020.
278. Yang, C. H.; Leon, R. C. C.; Hwang, J. C. C.; Saraiva, A.; Tanttu, T.; Huang, W.; Camirand Lemyre, J.; Chan, K. W.; Tan, K. Y.; Hudson, F. E.; Itoh, K. M.; Morello, A.; Pioro-Ladrière, M.; Laucht, A.; Dzurak, A. S. (April 2020). "Operation of a silicon quantum processor unit cell above one kelvin". *Nature*. **580** (7803): 350–354. arXiv:1902.09126 (https://arxiv.org/abs/1902.09126). Bibcode:2020Natur.580..350Y (https://ui.adsabs.harvard.edu/abs/2020Natur.580..350Y). doi:10.1038/s41586-020-2171-6 (https://doi.org/10.1038%2Fs41586-020-2171-6). PMID 32296190 (https://pubmed.ncbi.nlm.nih.gov/32296190). S2CID 119520750 (https://api.semanticscholar.org/CorpusID:119520750).
279. "New discovery settles long-standing debate about photovoltaic materials" (https://phys.org/news/2020-04-discovery-long-standing-debate-photovoltaic-materials.html). *phys.org*. Retrieved May 17, 2020.
280. Liu, Z.; Vaswani, C.; Yang, X.; Zhao, X.; Yao, Y.; Song, Z.; Cheng, D.; Shi, Y.; Luo, L.; Mudiyanselage, D.-H.; Huang, C.; Park, J.-M.; Kim, R. H. J.; Zhao, J.; Yan, Y.; Ho, K.-M.; Wang, J. (April 16, 2020). "Ultrafast Control of Excitonic Rashba Fine Structure by Phonon Coherence in the Metal Halide Perovskite $CH_3NH_3PbI_3$" (https://doi.org/10.1103%2FPhysRevLett.124.157401). *Physical Review Letters*. **124** (15): 157401. arXiv:1905.12373 (https://arxiv.org/abs/1905.12373). doi:10.1103/PhysRevLett.124.157401 (https://doi.org/10.1103%2FPhysRevLett.124.157401). PMID 32357060 (https://pubmed.ncbi.nlm.nih.gov/32357060). S2CID 214606050 (https://api.semanticscholar.org/CorpusID:214606050).
281. "Scientists demonstrate quantum radar prototype" (https://phys.org/news/2020-05-scientists-quantum-radar-prototype.html). *phys.org*. Retrieved June 12, 2020.
282. " 'Quantum radar' uses entangled photons to detect objects" (https://newatlas.com/physics/quantum-radar-entangled-photons/). *New Atlas*. May 12, 2020. Retrieved June 12, 2020.
283. Barzanjeh, S.; Pirandola, S.; Vitali, D.; Fink, J. M. (May 1, 2020). "Microwave quantum illumination using a digital receiver" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7272231). *Science Advances*. **6** (19): eabb0451. arXiv:1908.03058 (https://arxiv.org/abs/1908.03058). Bibcode:2020SciA....6..451B (https://ui.adsabs.harvard.edu/abs/2020SciA....6..451B). doi:10.1126/sciadv.abb0451 (https://doi.org/10.1126%2Fsciadv.abb0451). PMC 7272231 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7272231). PMID 32548249 (https://pubmed.ncbi.nlm.nih.gov/32548249).
284. "Scientists break the link between a quantum material's spin and orbital states" (https://phys.org/news/2020-05-scientists-link-quantum-material-orbital.html). *phys.org*. Retrieved June 12, 2020.
285. Shen, L.; Mack, S. A.; Dakovski, G.; Coslovich, G.; Krupin, O.; Hoffmann, M.; Huang, S.-W.; Chuang, Y-D.; Johnson, J. A.; Lieu, S.; Zohar, S.; Ford, C.; Kozina, M.; Schlotter, W.; Minitti, M. P.; Fujioka, J.; Moore, R.; Lee, W-S.; Hussain, Z.; Tokura, Y.; Littlewood, P.; Turner, J. J. (May 12, 2020). "Decoupling spin–orbital correlations in a layered manganite amidst ultrafast hybridized charge-transfer band excitation" (https://doi.org/10.1103%2FPhysRevB.101.201103). *Physical Review B*. **101** (20): 201103. arXiv:1912.10234 (https://arxiv.org/abs/1912.10234). Bibcode:2020PhRvB.101t1103S (https://ui.adsabs.harvard.edu/abs/2020PhRvB.101t1103S). doi:10.1103/PhysRevB.101.201103 (https://doi.org/10.1103%2FPhysRevB.101.201103).
286. "Photon discovery is a major step toward large-scale quantum technologies" (https://phys.org/news/2020-05-photon-discovery-major-large-scale-quantum.html). *phys.org*. Retrieved June 14, 2020.
287. "Physicists develop integrated photon source for macro quantum-photonics" (https://optics.org/news/11/5/44). *optics.org*. Retrieved June 14, 2020.

288. Paesani, S.; Borghi, M.; Signorini, S.; Maïnos, A.; Pavesi, L.; Laing, A. (May 19, 2020). "Near-ideal spontaneous photon sources in silicon quantum photonics" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7237445). *Nature Communications*. **11** (1): 2505. arXiv:2005.09579 (https://arxiv.org/abs/2005.09579). Bibcode:2020NatCo..11.2505P (https://ui.adsabs.harvard.edu/abs/2020NatCo..11.2505P). doi:10.1038/s41467-020-16187-8 (https://doi.org/10.1038%2Fs41467-020-16187-8). PMC 7237445 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7237445). PMID 32427911 (https://pubmed.ncbi.nlm.nih.gov/32427911).
289. Lachmann, Maike D.; Rasel, Ernst M. (June 11, 2020). "Quantum matter orbits Earth" (https://doi.org/10.1038%2Fd41586-020-01653-6). *Nature*. **582** (7811): 186–187. Bibcode:2020Natur.582..186L (https://ui.adsabs.harvard.edu/abs/2020Natur.582..186L). doi:10.1038/d41586-020-01653-6 (https://doi.org/10.1038%2Fd41586-020-01653-6). PMID 32528088 (https://pubmed.ncbi.nlm.nih.gov/32528088).
290. "Quantum 'fifth state of matter' observed in space for first time" (https://phys.org/news/2020-06-quantum-state-space.html). *phys.org*. Retrieved July 4, 2020.
291. Aveline, David C.; Williams, Jason R.; Elliott, Ethan R.; Dutenhoffer, Chelsea; Kellogg, James R.; Kohel, James M.; Lay, Norman E.; Oudrhiri, Kamal; Shotwell, Robert F.; Yu, Nan; Thompson, Robert J. (June 2020). "Observation of Bose–Einstein condensates in an Earth-orbiting research lab". *Nature*. **582** (7811): 193–197. Bibcode:2020Natur.582..193A (https://ui.adsabs.harvard.edu/abs/2020Natur.582..193A). doi:10.1038/s41586-020-2346-1 (https://doi.org/10.1038%2Fs41586-020-2346-1). PMID 32528092 (https://pubmed.ncbi.nlm.nih.gov/32528092). S2CID 219568565 (https://api.semanticscholar.org/CorpusID:219568565).
292. "The smallest motor in the world" (https://phys.org/news/2020-06-smallest-motor-world.html). *phys.org*. Retrieved July 4, 2020.
293. "Nano-motor of just 16 atoms runs at the boundary of quantum physics" (https://newatlas.com/physics/nano-motor-quantum-physics/). *New Atlas*. June 17, 2020. Retrieved July 4, 2020.
294. Stolz, Samuel; Gröning, Oliver; Prinz, Jan; Brune, Harald; Widmer, Roland (June 15, 2020). "Molecular motor crossing the frontier of classical to quantum tunneling motion" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7334648). *Proceedings of the National Academy of Sciences*. **117** (26): 14838–14842. Bibcode:2020PNAS..11714838S (https://ui.adsabs.harvard.edu/abs/2020PNAS..11714838S). doi:10.1073/pnas.1918654117 (https://doi.org/10.1073%2Fpnas.1918654117). ISSN 0027-8424 (https://search.worldcat.org/issn/0027-8424). PMC 7334648 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7334648). PMID 32541061 (https://pubmed.ncbi.nlm.nih.gov/32541061).
295. "New techniques improve quantum communication, entangle phonons" (https://phys.org/news/2020-06-techniques-quantum-entangle-phonons.html). *phys.org*. Retrieved July 5, 2020.
296. Schirber, Michael (June 12, 2020). "Quantum Erasing with Phonons" (https://physics.aps.org/articles/v13/95). *Physics*. Retrieved July 5, 2020.
297. Chang, H.-S.; Zhong, Y. P.; Bienfait, A.; Chou, M.-H.; Conner, C. R.; Dumur, É.; Grebel, J.; Peairs, G. A.; Povey, R. G.; Satzinger, K. J.; Cleland, A. N. (June 17, 2020). "Remote Entanglement via Adiabatic Passage Using a Tunably Dissipative Quantum Communication System". *Physical Review Letters*. **124** (24): 240502. arXiv:2005.12334 (https://arxiv.org/abs/2005.12334). Bibcode:2020PhRvL.124x0502C (https://ui.adsabs.harvard.edu/abs/2020PhRvL.124x0502C). doi:10.1103/PhysRevLett.124.240502 (https://doi.org/10.1103%2FPhysRevLett.124.240502). PMID 32639797 (https://pubmed.ncbi.nlm.nih.gov/32639797). S2CID 218889298 (https://api.semanticscholar.org/CorpusID:218889298).
298. Bienfait, A.; Zhong, Y. P.; Chang, H.-S.; Chou, M.-H.; Conner, C. R.; Dumur, É.; Grebel, J.; Peairs, G. A.; Povey, R. G.; Satzinger, K. J.; Cleland, A. N. (June 12, 2020). "Quantum Erasure Using Entangled Surface Acoustic Phonons" (https://doi.org/10.1103%2FPhysRevX.10.021055). *Physical Review X*. **10** (2): 021055. arXiv:2005.09311 (https://arxiv.org/abs/2005.09311). Bibcode:2020PhRvX..10b1055B (https://ui.adsabs.harvard.edu/abs/2020PhRvX..10b1055B). doi:10.1103/PhysRevX.10.021055 (https://doi.org/10.1103%2FPhysRevX.10.021055).

299. "Honeywell claims to have world's highest performing quantum computer according to IBM's benchmark" (https://www.zdnet.com/article/honeywell-claims-to-have-worlds-highest-performing-quantum-computer-according-to-ibms-benchmark/?_amp_linker=1%2a1ms9d9v%2aid%2aVUpFdHE1cVlKZ2pMd0ZBaWNVVlgwSkFIODZKRFlianMwVEwzRVdRMFF4Z1N1cHlfRVZvXzQzbk1Wc1JLODMwZw..#ftag=CAD-00-10aag7e). *ZDNet*.
300. "UChicago scientists discover way to make quantum states last 10,000 times longer" (https://www.anl.gov/article/uchicago-scientists-discover-way-to-make-quantum-states-last-10000-times-longer). *Argonne National Laboratory*. August 13, 2020. Retrieved August 14, 2020.
301. Miao, Kevin C.; Blanton, Joseph P.; Anderson, Christopher P.; Bourassa, Alexandre; Crook, Alexander L.; Wolfowicz, Gary; Abe, Hiroshi; Ohshima, Takeshi; Awschalom, David D. (May 12, 2020). "Universal coherence protection in a solid-state spin qubit". *Science*. **369** (6510): 1493–1497. arXiv:2005.06082v1 (https://arxiv.org/abs/2005.06082v1). Bibcode:2020Sci...369.1493M (https://ui.adsabs.harvard.edu/abs/2020Sci...369.1493M). doi:10.1126/science.abc5186 (https://doi.org/10.1126%2Fscience.abc5186). PMID 32792463 (https://pubmed.ncbi.nlm.nih.gov/32792463). S2CID 218613907 (https://api.semanticscholar.org/CorpusID:218613907).
302. "Quantum computers may be destroyed by high-energy particles from space" (https://www.newscientist.com/article/2252933-quantum-computers-may-be-destroyed-by-high-energy-particles-from-space/). *New Scientist*. Retrieved September 7, 2020.
303. "Cosmic rays may soon stymie quantum computing" (https://phys.org/news/2020-08-cosmic-rays-stymie-quantum.html). *phys.org*. Retrieved September 7, 2020.
304. Vepsäläinen, Antti P.; Karamlou, Amir H.; Orrell, John L.; Dogra, Akshunna S.; Loer, Ben; Vasconcelos, Francisca; Kim, David K.; Melville, Alexander J.; Niedzielski, Bethany M.; Yoder, Jonilyn L.; Gustavsson, Simon; Formaggio, Joseph A.; VanDevender, Brent A.; Oliver, William D. (August 2020). "Impact of ionizing radiation on superconducting qubit coherence" (https://www.nature.com/articles/s41586-020-2619-8). *Nature*. **584** (7822): 551–556. arXiv:2001.09190 (https://arxiv.org/abs/2001.09190). Bibcode:2020Natur.584..551V (https://ui.adsabs.harvard.edu/abs/2020Natur.584..551V). doi:10.1038/s41586-020-2619-8 (https://doi.org/10.1038%2Fs41586-020-2619-8). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 32848227 (https://pubmed.ncbi.nlm.nih.gov/32848227). S2CID 210920566 (https://api.semanticscholar.org/CorpusID:210920566). Retrieved September 7, 2020.
305. "Google conducts largest chemical simulation on a quantum computer to date" (https://phys.org/news/2020-08-google-largest-chemical-simulation-quantum.html). *phys.org*. Retrieved September 7, 2020.
306. Savage, Neil. "Google's Quantum Computer Achieves Chemistry Milestone" (https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/). *Scientific American*. Retrieved September 7, 2020.
307. Arute, Frank; et al. (Google AI Quantum Collaborators) (August 28, 2020). "Hartree–Fock on a superconducting qubit quantum computer" (https://www.science.org/doi/10.1126/science.abb9811). *Science*. **369** (6507): 1084–1089. arXiv:2004.04174 (https://arxiv.org/abs/2004.04174). Bibcode:2020Sci...369.1084. (https://ui.adsabs.harvard.edu/abs/2020Sci...369.1084.). doi:10.1126/science.abb9811 (https://doi.org/10.1126%2Fscience.abb9811). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 32855334 (https://pubmed.ncbi.nlm.nih.gov/32855334). S2CID 215548188 (https://api.semanticscholar.org/CorpusID:215548188). Retrieved September 7, 2020.
308. "Multi-user communication network paves the way towards the quantum internet" (https://physicsworld.com/a/multi-user-communication-network-paves-the-way-towards-the-quantum-internet/). *Physics World*. September 8, 2020. Retrieved October 8, 2020.

309. Joshi, Siddarth Koduru; Aktas, Djeylan; Wengerowsky, Sören; Lončarić, Martin; Neumann, Sebastian Philipp; Liu, Bo; Scheidl, Thomas; Lorenzo, Guillermo Currás; Samec, Željko; Kling, Laurent; Qiu, Alex; Razavi, Mohsen; Stipčević, Mario; Rarity, John G.; Ursin, Rupert (September 1, 2020). "A trusted node–free eight-user metropolitan quantum communication network" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7467697). *Science Advances*. **6** (36): eaba0959. arXiv:1907.08229 (https://arxiv.org/abs/1907.08229). Bibcode:2020SciA....6..959J (https://ui.adsabs.harvard.edu/abs/2020SciA....6..959J). doi:10.1126/sciadv.aba0959 (https://doi.org/10.1126%2Fsciadv.aba0959). ISSN 2375-2548 (https://search.worldcat.org/issn/2375-2548). PMC 7467697 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7467697). PMID 32917585 (https://pubmed.ncbi.nlm.nih.gov/32917585). Text and images are available under a Creative Commons Attribution 4.0 International License.
310. "First Photonic Quantum Computer on the Cloud – IEEE Spectrum" (https://spectrum.ieee.org/photonic-quantum).
311. "Quantum entanglement realized between distant large objects" (https://phys.org/news/2020-09-quantum-entanglement-distant-large.html). *phys.org*. Retrieved October 9, 2020.
312. Thomas, Rodrigo A.; Parniak, Michał; Østfeldt, Christoffer; Møller, Christoffer B.; Bærentsen, Christian; Tsaturyan, Yeghishe; Schliesser, Albert; Appel, Jürgen; Zeuthen, Emil; Polzik, Eugene S. (September 21, 2020). "Entanglement between distant macroscopic mechanical and spin systems" (https://www.nature.com/articles/s41567-020-1031-5). *Nature Physics*. **17** (2): 228–233. arXiv:2003.11310 (https://arxiv.org/abs/2003.11310). doi:10.1038/s41567-020-1031-5 (https://doi.org/10.1038%2Fs41567-020-1031-5). ISSN 1745-2481 (https://search.worldcat.org/issn/1745-2481). S2CID 214641162 (https://api.semanticscholar.org/CorpusID:214641162). Retrieved October 9, 2020.
313. "Chinese team unveils exceedingly fast quantum computer" (http://global.chinadaily.com.cn/a/202012/04/WS5fc96deba31024ad0ba99abf.html). *China Daily*. December 4, 2020. Retrieved December 5, 2020.
314. "China Stakes Its Claim to Quantum Supremacy" (https://www.wired.com/story/china-stakes-claim-quantum-supremacy/). *Wired*. December 3, 2020. Retrieved December 5, 2020.
315. Zhong, Han-Sen; Wang, Hui; Deng, Yu-Hao; Chen, Ming-Cheng; Peng, Li-Chao; Luo, Yi-Han; Qin, Jian; Wu, Dian; Ding, Xing; Hu, Yi; Hu, Peng; Yang, Xiao-Yan; Zhang, Wei-Jun; Li, Hao; Li, Yuxuan; Jiang, Xiao; Gan, Lin; Yang, Guangwen; You, Lixing; Wang, Zhen; Li, Li; Liu, Nai-Le; Lu, Chao-Yang; Pan, Jian-Wei (December 18, 2020). "Quantum computational advantage using photons" (https://www.science.org/doi/full/10.1126/science.abe8770). *Science*. **370** (6523): 1460–1463. arXiv:2012.01625 (https://arxiv.org/abs/2012.01625). Bibcode:2020Sci...370.1460Z (https://ui.adsabs.harvard.edu/abs/2020Sci...370.1460Z). doi:10.1126/science.abe8770 (https://doi.org/10.1126%2Fscience.abe8770). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33273064 (https://pubmed.ncbi.nlm.nih.gov/33273064). S2CID 227254333 (https://api.semanticscholar.org/CorpusID:227254333). Retrieved January 22, 2021.
316. "Honeywell introduces quantum computing as a service with subscription offering" (https://www.zdnet.com/article/honeywell-introduces-quantum-computing-as-a-service-with-subscription-offering/#ftag=CAD-00-10aag7e). *ZDNet*.
317. "Three Frosty Innovations for Better Quantum Computers – IEEE Spectrum" (https://spectrum.ieee.org/three-super-cold-devices-quantum-computers).
318. "Scientists Achieve Direct Counterfactual Quantum Communication For The First Time" (https://futurism.com/scientists-achieve-direct-counterfactual-quantum-communication-for-the-first-time). *Futurism*. Retrieved January 16, 2021.
319. "Elementary particles part ways with their properties" (https://phys.org/news/2020-12-elementary-particles-ways-properties.html). *phys.org*. Retrieved January 16, 2021.
320. McRae, Mike. "In a Mind-Bending New Paper, Physicists Give Schrodinger's Cat a Cheshire Grin" (https://www.sciencealert.com/schrodinger-s-cat-gets-a-cheshire-grin-in-a-mind-bending-quantum-physics-analysis). *ScienceAlert*. Retrieved January 16, 2021.

321. Aharonov, Yakir; Rohrlich, Daniel (December 21, 2020). "What Is Nonlocal in Counterfactual Quantum Communication?" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.125.260401). *Physical Review Letters*. **125** (26): 260401. arXiv:2011.11667 (https://arxiv.org/abs/2011.11667). Bibcode:2020PhRvL.125z0401A (https://ui.adsabs.harvard.edu/abs/2020PhRvL.125z0401A). doi:10.1103/PhysRevLett.125.260401 (https://doi.org/10.1103%2FPhysRevLett.125.260401). PMID 33449741 (https://pubmed.ncbi.nlm.nih.gov/33449741). S2CID 145994494 (https://api.semanticscholar.org/CorpusID:145994494). Retrieved January 16, 2021. Available under CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/).
322. "The world's first integrated quantum communication network" (https://phys.org/news/2021-01-world-quantum-network.html). *phys.org*. Retrieved February 11, 2021.
323. Chen, Yu-Ao; Zhang, Qiang; Chen, Teng-Yun; Cai, Wen-Qi; Liao, Sheng-Kai; Zhang, Jun; Chen, Kai; Yin, Juan; Ren, Ji-Gang; Chen, Zhu; Han, Sheng-Long; Yu, Qing; Liang, Ken; Zhou, Fei; Yuan, Xiao; Zhao, Mei-Sheng; Wang, Tian-Yin; Jiang, Xiao; Zhang, Liang; Liu, Wei-Yue; Li, Yang; Shen, Qi; Cao, Yuan; Lu, Chao-Yang; Shu, Rong; Wang, Jian-Yu; Li, Li; Liu, Nai-Le; Xu, Feihu; Wang, Xiang-Bin; Peng, Cheng-Zhi; Pan, Jian-Wei (January 2021). "An integrated space-to-ground quantum communication network over 4,600 kilometres" (https://www.nature.com/articles/s41586-020-03093-8). *Nature*. **589** (7841): 214–219. Bibcode:2021Natur.589..214C (https://ui.adsabs.harvard.edu/abs/2021Natur.589..214C). doi:10.1038/s41586-020-03093-8 (https://doi.org/10.1038%2Fs41586-020-03093-8). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 33408416 (https://pubmed.ncbi.nlm.nih.gov/33408416). S2CID 230812317 (https://api.semanticscholar.org/CorpusID:230812317). Retrieved February 11, 2021.
324. "Error-protected quantum bits entangled for the first time" (https://phys.org/news/2021-01-error-protected-quantum-bits-entangled.html). *phys.org*. Retrieved August 30, 2021.
325. Erhard, Alexander; Poulsen Nautrup, Hendrik; Meth, Michael; Postler, Lukas; Stricker, Roman; Stadler, Martin; Negnevitsky, Vlad; Ringbauer, Martin; Schindler, Philipp; Briegel, Hans J.; Blatt, Rainer; Friis, Nicolai; Monz, Thomas (January 2021). "Entangling logical qubits with lattice surgery" (https://www.nature.com/articles/s41586-020-03079-6). *Nature*. **589** (7841): 220–224. arXiv:2006.03071 (https://arxiv.org/abs/2006.03071). Bibcode:2021Natur.589..220E (https://ui.adsabs.harvard.edu/abs/2021Natur.589..220E). doi:10.1038/s41586-020-03079-6 (https://doi.org/10.1038%2Fs41586-020-03079-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 33442044 (https://pubmed.ncbi.nlm.nih.gov/33442044). S2CID 219401398 (https://api.semanticscholar.org/CorpusID:219401398). Retrieved August 30, 2021.
326. "Using drones to create local quantum networks" (https://phys.org/news/2021-01-drones-local-quantum-networks.html). *phys.org*. Retrieved February 12, 2021.
327. Liu, Hua-Ying; Tian, Xiao-Hui; Gu, Changsheng; Fan, Pengfei; Ni, Xin; Yang, Ran; Zhang, Ji-Ning; Hu, Mingzhe; Guo, Jian; Cao, Xun; Hu, Xiaopeng; Zhao, Gang; Lu, Yan-Qing; Gong, Yan-Xiao; Xie, Zhenda; Zhu, Shi-Ning (January 15, 2021). "Optical-Relayed Entanglement Distribution Using Drones as Mobile Nodes" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.126.020503). *Physical Review Letters*. **126** (2): 020503. Bibcode:2021PhRvL.126b0503L (https://ui.adsabs.harvard.edu/abs/2021PhRvL.126b0503L). doi:10.1103/PhysRevLett.126.020503 (https://doi.org/10.1103%2FPhysRevLett.126.020503). PMID 33512193 (https://pubmed.ncbi.nlm.nih.gov/33512193). S2CID 231761406 (https://api.semanticscholar.org/CorpusID:231761406). Retrieved February 12, 2021.
328. "BMW explores quantum computing to boost supply chain efficiencies" (https://www.zdnet.com/article/bmw-explores-quantum-computing-to-boost-supply-chain-efficiencies/#ftag=CAD-00-10aag7e). *ZDNet*.
329. "Physicists develop record-breaking source for single photons" (https://phys.org/news/2021-01-physicists-record-breaking-source-photons.html). *phys.org*. Retrieved February 12, 2021.

330. Tomm, Natasha; Javadi, Alisa; Antoniadis, Nadia Olympia; Najer, Daniel; Löbl, Matthias Christian; Korsch, Alexander Rolf; Schott, Rüdiger; Valentin, Sascha René; Wieck, Andreas Dirk; Ludwig, Arne; Warburton, Richard John (January 28, 2021). "A bright and fast source of coherent single photons" (https://www.nature.com/articles/s41565-020-00831-x). *Nature Nanotechnology*. **16** (4): 399–403. arXiv:2007.12654 (https://arxiv.org/abs/2007.12654). Bibcode:2021NatNa..16..399T (https://ui.adsabs.harvard.edu/abs/2021NatNa..16..399T). doi:10.1038/s41565-020-00831-x (https://doi.org/10.1038%2Fs41565-020-00831-x). ISSN 1748-3395 (https://search.worldcat.org/issn/1748-3395). PMID 33510454 (https://pubmed.ncbi.nlm.nih.gov/33510454). S2CID 220769410 (https://api.semanticscholar.org/CorpusID:220769410). Retrieved February 12, 2021.
331. "You can now try out a quantum computer with Microsoft's Azure cloud service" (https://www.cnet.com/tech/computing/microsoft-opens-its-azure-quantum-computer-cloud-service-to-the-public/).
332. "Quantum systems learn joint computing" (https://phys.org/news/2021-02-quantum-joint.html). *phys.org*. Retrieved March 7, 2021.
333. Daiss, Severin; Langenfeld, Stefan; Welte, Stephan; Distante, Emanuele; Thomas, Philip; Hartung, Lukas; Morin, Olivier; Rempe, Gerhard (February 5, 2021). "A quantum-logic gate between distant quantum-network modules" (https://www.science.org/doi/10.1126/science.abe3150). *Science*. **371** (6529): 614–617. arXiv:2103.13095 (https://arxiv.org/abs/2103.13095). Bibcode:2021Sci...371..614D (https://ui.adsabs.harvard.edu/abs/2021Sci...371..614D). doi:10.1126/science.abe3150 (https://doi.org/10.1126%2Fscience.abe3150). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33542133 (https://pubmed.ncbi.nlm.nih.gov/33542133). S2CID 231808141 (https://api.semanticscholar.org/CorpusID:231808141). Retrieved March 7, 2021.
334. "Quantum computing: Honeywell just quadrupled the power of its computer" (https://www.zdnet.com/article/quantum-computing-honeywell-just-quadrupled-the-power-of-its-computer/). *ZDNet*.
335. "We could detect alien civilizations through their interstellar quantum communication" (https://phys.org/news/2021-04-alien-civilizations-interstellar-quantum.html). *phys.org*. Retrieved May 9, 2021.
336. Hippke, Michael (April 13, 2021). "Searching for Interstellar Quantum Communications" (https://doi.org/10.3847%2F1538-3881%2Fabf7b7). *The Astronomical Journal*. **162** (1): 1. arXiv:2104.06446 (https://arxiv.org/abs/2104.06446). Bibcode:2021AJ....162....1H (https://ui.adsabs.harvard.edu/abs/2021AJ....162....1H). doi:10.3847/1538-3881/abf7b7 (https://doi.org/10.3847%2F1538-3881%2Fabf7b7). S2CID 233231350 (https://api.semanticscholar.org/CorpusID:233231350).
337. "Vibrating drumheads are entangled quantum mechanically" (https://physicsworld.com/a/vibrating-drumheads-are-entangled-quantum-mechanically/). *Physics World*. May 17, 2021. Retrieved June 14, 2021.
338. Lépinay, Laure Mercier de; Ockeloen-Korppi, Caspar F.; Woolley, Matthew J.; Sillanpää, Mika A. (May 7, 2021). "Quantum mechanics–free subsystem with mechanical oscillators" (https://www.science.org/doi/10.1126/science.abf5389). *Science*. **372** (6542): 625–629. arXiv:2009.12902 (https://arxiv.org/abs/2009.12902). Bibcode:2021Sci...372..625M (https://ui.adsabs.harvard.edu/abs/2021Sci...372..625M). doi:10.1126/science.abf5389 (https://doi.org/10.1126%2Fscience.abf5389). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33958476 (https://pubmed.ncbi.nlm.nih.gov/33958476). S2CID 221971015 (https://api.semanticscholar.org/CorpusID:221971015). Retrieved June 14, 2021.

339. Kotler, Shlomi; Peterson, Gabriel A.; Shojaee, Ezad; Lecocq, Florent; Cicak, Katarina; Kwiatkowski, Alex; Geller, Shawn; Glancy, Scott; Knill, Emanuel; Simmonds, Raymond W.; Aumentado, José; Teufel, John D. (May 7, 2021). "Direct observation of deterministic macroscopic entanglement" (https://www.science.org/doi/10.1126/science.abf2998). *Science*. **372** (6542): 622–625. arXiv:2004.05515 (https://arxiv.org/abs/2004.05515). Bibcode:2021Sci...372..622K (https://ui.adsabs.harvard.edu/abs/2021Sci...372..622K). doi:10.1126/science.abf2998 (https://doi.org/10.1126%2Fscience.abf2998). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33958475 (https://pubmed.ncbi.nlm.nih.gov/33958475). S2CID 233872863 (https://api.semanticscholar.org/CorpusID:233872863). Retrieved June 14, 2021.
340. "TOSHIBA ANNOUNCES BREAKTHROUGH IN LONG DISTANCE QUANTUM COMMUNICATION" (https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/toshiba-announces-breakthrough-in-long-distance-quantum-communication). *Toshiba*. June 12, 2021. Retrieved June 12, 2021.
341. "Researchers create an 'un-hackable' quantum network over hundreds of kilometers using optical fiber" (https://www.zdnet.com/article/researchers-created-an-un-hackable-quantum-network-over-hundreds-of-kilometers-using-optical-fiber/). *ZDNet*. June 8, 2021. Retrieved June 12, 2021.
342. Pittaluga, Mirko; Minder, Mariella; Lucamarini, Marco; Sanzaro, Mirko; Woodward, Robert I.; Li, Ming-Jun; Yuan, Zhiliang; Shields, Andrew J. (July 2021). "600-km repeater-like quantum communications with dual-band stabilization" (https://www.nature.com/articles/s41566-021-00811-0). *Nature Photonics*. **15** (7): 530–535. arXiv:2012.15099 (https://arxiv.org/abs/2012.15099). Bibcode:2021NaPho..15..530P (https://ui.adsabs.harvard.edu/abs/2021NaPho..15..530P). doi:10.1038/s41566-021-00811-0 (https://doi.org/10.1038%2Fs41566-021-00811-0). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893). S2CID 229923162 (https://api.semanticscholar.org/CorpusID:229923162). Retrieved July 19, 2021.
343. "Quantum computer is smallest ever, claim physicists" (https://physicsworld.com/a/quantum-computer-is-smallest-ever-claim-physicists/). *Physics World*. July 7, 2021. Retrieved July 11, 2021.
344. Pogorelov, I.; Feldker, T.; Marciniak, Ch. D.; Postler, L.; Jacob, G.; Krieglsteiner, O.; Podlesnic, V.; Meth, M.; Negnevitsky, V.; Stadler, M.; Höfer, B.; Wächter, C.; Lakhmanskiy, K.; Blatt, R.; Schindler, P.; Monz, T. (June 17, 2021). "Compact Ion-Trap Quantum Computing Demonstrator" (https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.2.020343). *PRX Quantum*. **2** (2): 020343. arXiv:2101.11390 (https://arxiv.org/abs/2101.11390). Bibcode:2021PRXQ....2b0343P (https://ui.adsabs.harvard.edu/abs/2021PRXQ....2b0343P). doi:10.1103/PRXQuantum.2.020343 (https://doi.org/10.1103%2FPRXQuantum.2.020343). S2CID 231719119 (https://api.semanticscholar.org/CorpusID:231719119). Retrieved July 11, 2021.
345. "IBM researchers demonstrate the advantage that quantum computers have over classical computers" (https://www.zdnet.com/article/ibm-researchers-demonstrate-the-advantage-that-quantum-computers-have-over-classical-computers/?ftag=TRE-03-10aaa6b&bhid=28974009886604832149562936007498&mid=13420444&cid=2193388821&eh=70013a02f0e22ff3dec6ccb58d5e95e4e57150473218ab3ecaf4d84e5143828a). *ZDNet*.
346. "Bigger quantum computers, faster: This new idea could be the quickest route to real world apps" (https://www.zdnet.com/article/quantum-computing-this-new-approach-could-be-the-fastest-path-to-real-applications/?ftag=TRE-03-10aaa6b&bhid=28974009886604832149562936007498&mid=13420444&cid=2193388821&eh=70013a02f0e22ff3dec6ccb58d5e95e4e57150473218ab3ecaf4d84e5143828a). *ZDNet*.
347. "Harvard-led physicists take big step in race to quantum computing" (https://scienmag.com/harvard-led-physicists-take-big-step-in-race-to-quantum-computing/). *Scienmag: Latest Science and Health News*. July 9, 2021. Retrieved August 14, 2021.

348. Ebadi, Sepehr; Wang, Tout T.; Levine, Harry; Keesling, Alexander; Semeghini, Giulia; Omran, Ahmed; Bluvstein, Dolev; Samajdar, Rhine; Pichler, Hannes; Ho, Wen Wei; Choi, Soonwon; Sachdev, Subir; Greiner, Markus; Vuletić, Vladan; Lukin, Mikhail D. (July 2021). "Quantum phases of matter on a 256-atom programmable quantum simulator". *Nature*. **595** (7866): 227–232. arXiv:2012.12281 (https://arxiv.org/abs/2012.12281). Bibcode:2021Natur.595..227E (https://ui.adsabs.harvard.edu/abs/2021Natur.595..227E). doi:10.1038/s41586-021-03582-4 (https://doi.org/10.1038%2Fs41586-021-03582-4). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 34234334 (https://pubmed.ncbi.nlm.nih.gov/34234334). S2CID 229363764 (https://api.semanticscholar.org/CorpusID:229363764).
349. Scholl, Pascal; Schuler, Michael; Williams, Hannah J.; Eberharter, Alexander A.; Barredo, Daniel; Schymik, Kai-Niklas; Lienhard, Vincent; Henry, Louis-Paul; Lang, Thomas C.; Lahaye, Thierry; Läuchli, Andreas M. (July 7, 2021). "Quantum simulation of 2D antiferromagnets with hundreds of Rydberg atoms" (https://www.nature.com/articles/s41586-021-03585-1). *Nature*. **595** (7866): 233–238. arXiv:2012.12268 (https://arxiv.org/abs/2012.12268). Bibcode:2021Natur.595..233S (https://ui.adsabs.harvard.edu/abs/2021Natur.595..233S). doi:10.1038/s41586-021-03585-1 (https://doi.org/10.1038%2Fs41586-021-03585-1). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 34234335 (https://pubmed.ncbi.nlm.nih.gov/34234335). S2CID 229363462 (https://api.semanticscholar.org/CorpusID:229363462).
350. "China quantum computers are 1 million times more powerful Google's" (https://techhq.com/2021/10/china-has-quantum-computers-that-are-a-million-times-more-powerful-than-googles/). *TechHQ*. October 28, 2021. Retrieved November 16, 2021.
351. "China's quantum computing efforts surpasses the West's again" (https://techwireasia.com/2021/11/chinas-quantum-computing-efforts-surpasses-the-wests-yet-again/). *Tech Wire Asia*. November 3, 2021. Retrieved November 16, 2021.
352. "Canadian researchers achieve first quantum simulation of baryons" (https://uwaterloo.ca/news/media/canadian-researchers-achieve-first-quantum-simulation). *University of Waterloo*. November 11, 2021. Retrieved November 12, 2021.
353. Atas, Yasar Y.; Zhang, Jinglei; Lewis, Randy; Jahanpour, Amin; Haase, Jan F.; Muschik, Christine A. (November 11, 2021). "SU(2) hadrons on a quantum computer via a variational approach" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8586147). *Nature Communications*. **12** (1): 6499. Bibcode:2021NatCo..12.6499A (https://ui.adsabs.harvard.edu/abs/2021NatCo..12.6499A). doi:10.1038/s41467-021-26825-4 (https://doi.org/10.1038%2Fs41467-021-26825-4). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 8586147 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8586147). PMID 34764262 (https://pubmed.ncbi.nlm.nih.gov/34764262).
354. "IBM creates largest ever superconducting quantum computer" (https://www.newscientist.com/article/2297583-ibm-creates-largest-ever-superconducting-quantum-computer/). *New Scientist*. Retrieved February 12, 2022.
355. "IBM Unveils Breakthrough 127-Qubit Quantum Processor" (https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor). *IBM Newsroom*. Retrieved January 12, 2022.
356. "Europe's First Quantum Computer with More Than 5K Qubits Launched at Jülich" (https://www.hpcwire.com/off-the-wire/europes-first-quantum-computer-with-more-than-5k-qubits-launched-at-julich/). *HPC Wire*. January 18, 2022. Archived (https://web.archive.org/web/20220120070625/https://www.hpcwire.com/off-the-wire/europes-first-quantum-computer-with-more-than-5k-qubits-launched-at-julich/) from the original on January 20, 2022. Retrieved January 20, 2022.
357. "Artificial neurons go quantum with photonic circuits" (https://phys.org/news/2022-03-artificial-neurons-quantum-photonic-circuits.html). *University of Vienna*. Retrieved April 19, 2022.

358. Spagnolo, Michele; Morris, Joshua; Piacentini, Simone; Antesberger, Michael; Massa, Francesco; Crespi, Andrea; Ceccarelli, Francesco; Osellame, Roberto; Walther, Philip (April 2022). "Experimental photonic quantum memristor". *Nature Photonics*. **16** (4): 318–323. arXiv:2105.04867 (https://arxiv.org/abs/2105.04867). Bibcode:2022NaPho..16..318S (https://ui.adsabs.harvard.edu/abs/2022NaPho..16..318S). doi:10.1038/s41566-022-00973-5 (https://doi.org/10.1038%2Fs41566-022-00973-5). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893). S2CID 234358015 (https://api.semanticscholar.org/CorpusID:234358015).
359. "Quantinuum Announces Quantum Volume 4096 Achievement" (https://www.quantinuum.com/pressrelease/quantinuum-announces-quantum-volume-4096-achievement). *www.quantinuum.com*. April 14, 2022. Retrieved May 2, 2022.
360. Universität Innsbruck (May 27, 2022). "Error-Free Quantum Computing Gets Real" (https://www.uibk.ac.at/en/newsroom/2022/error-free-quantum-computing-gets-real/). *www.uibk.ac.at*. Retrieved February 13, 2023.
361. "A Huge Step Forward in Quantum Computing Was Just Announced: The First-Ever Quantum Circuit" (https://www.sciencealert.com/a-huge-step-forward-in-quantum-computing-was-just-announced-the-first-ever-quantum-circuit). *Science Alert*. June 22, 2022. Retrieved June 23, 2022.
362. Kiczynski, M.; Gorman, S. K.; Geng, H.; Donnelly, M. B.; Chung, Y.; He, Y.; Keizer, J. G.; Simmons, M. Y. (June 2022). "Engineering topological states in atom-based semiconductor quantum dots" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9217742). *Nature*. **606** (7915): 694–699. Bibcode:2022Natur.606..694K (https://ui.adsabs.harvard.edu/abs/2022Natur.606..694K). doi:10.1038/s41586-022-04706-0 (https://doi.org/10.1038%2Fs41586-022-04706-0). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9217742 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9217742). PMID 35732762 (https://pubmed.ncbi.nlm.nih.gov/35732762).
    - Press release: "UNSW quantum scientists deliver world's first integrated circuit at the atomic scale" (https://newsroom.unsw.edu.au/news/science-tech/unsw-quantum-scientists-deliver-world%E2%80%99s-first-integrated-circuit-atomic-scale). *University of New South Wales*. June 23, 2022. Retrieved June 23, 2022.
363. Conover, Emily (July 5, 2022). "Aliens could send quantum messages to Earth, calculations suggest" (https://www.sciencenews.org/article/alien-quantum-communication-extraterrestrial-communication-signal). *Science News*. Retrieved July 13, 2022.
364. Berera, Arjun; Calderón-Figueroa, Jaime (June 28, 2022). "Viability of quantum communication across interstellar distances". *Physical Review D*. **105** (12): 123033. arXiv:2205.11816 (https://arxiv.org/abs/2205.11816). Bibcode:2022PhRvD.105l3033B (https://ui.adsabs.harvard.edu/abs/2022PhRvD.105l3033B). doi:10.1103/PhysRevD.105.123033 (https://doi.org/10.1103%2FPhysRevD.105.123033). S2CID 249017926 (https://api.semanticscholar.org/CorpusID:249017926).
365. Universität Innsbruck (July 21, 2022). "Quantum computer works with more than zero and one" (https://www.uibk.ac.at/en/newsroom/2022/quantum-computer-works-with-more-than-zero-and-one/). *www.uibk.ac.at*. Retrieved February 13, 2023.
366. Purdue University (August 15, 2022). "2D array of electron and nuclear spin qubits opens new frontier in quantum science" (https://phys.org/news/2022-08-2d-array-electron-nuclear-qubits.amp). Phys.org.
367. Max Planck Society (August 24, 2022). "Physicists entangle more than a dozen photons efficiently" (https://phys.org/news/2022-08-physicists-entangle-dozen-photons-efficiently.amp). *Nature*. **608** (7924). Phys.org: 677–681. doi:10.1038/s41586-022-04987-5 (https://doi.org/10.1038%2Fs41586-022-04987-5). PMC 9402438 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9402438). PMID 36002484 (https://pubmed.ncbi.nlm.nih.gov/36002484). Retrieved August 25, 2022.

368. Ritter, Florian; Max Planck Society. "Metasurfaces offer new possibilities for quantum research" (https://phys.org/news/2022-08-metasurfaces-possibilities-quantum.amp). Phys.org.
369. McRae, Mike (August 31, 2022). "Quantum Physicists Set New Record For Entangling Photons Together" (https://www.sciencealert.com/quantum-physicists-set-new-record-for-entangling-photons-together). *Science Alert*.
370. National Institute of Information and Communications Technology (September 2, 2022). "New method to systematically find optimal quantum operation sequences for quantum computers" (https://archive.today/20220904164853/https://phys.org/news/2022-09-method-systematically-optimal-quantum-sequences.amp). Phys.org. Archived from the original on September 4, 2022. Retrieved September 8, 2023.
371. University of New South Wales (September 30, 2022). "For the longest time: Quantum computing engineers set new standard in silicon chip performance" (https://archive.today/20221001222634/https://phys.org/news/2022-09-longest-quantum-standard-silicon-chip.amp). *Science Advances*. **7** (33). Phys.org. doi:10.1126/sciadv.abg9158 (https://doi.org/10.1126%2Fsciadv.abg9158). PMC 8363148 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8363148). PMID 34389538 (https://pubmed.ncbi.nlm.nih.gov/34389538). Archived from the original on October 1, 2022. Retrieved September 8, 2023.
372. "IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two" (https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two). *IBM*. November 9, 2022. Retrieved November 10, 2022.
373. "IBM unveils its 433 qubit Osprey quantum computer" (https://techcrunch.com/2022/11/09/ibm-unveils-its-433-qubit-osprey-quantum-computer/). *Tech Crunch*. November 9, 2022. Retrieved November 10, 2022.
374. "SpinQ Introduces Trio of Portable Quantum Computers" (https://www.tomshardware.com/news/spinq-introduces-trio-of-portable-quantum-computers). December 15, 2022. Retrieved December 15, 2022.
375. "World's first portable quantum computers on sale in Japan: Prices start at $8,700" (https://tech.news.am/eng/news/510/worlds-first-portable-quantum-computers-on-sale-in-japan-prices-start-at-$8700.html).
376. "Il futuro è ora: I primi computer quantistici portatili arrivano sul mercato" (https://translate.google.com/translate?sl=it&tl=en&hl=it&u=https://www.futuroprossimo.it/2023/05/il-futuro-e-ora-i-primi-computer-quantistici-portatili-in-vendita-in-giappone/amp/&client=webapp) [The future is now: The first portable quantum computers hit the market] (in Italian). May 19, 2023.
377. Universität Innsbruck (February 3, 2023). "Entangled atoms across the Innsbruck quantum network" (https://www.uibk.ac.at/en/newsroom/2023/entangled-atoms-across-the-innsbruck-quantum-network/). *www.uibk.ac.at*. Retrieved February 13, 2023.
378. AQT (February 8, 2023). "State of Quantum Computing in Europe: AQT pushing performance with a Quantum Volume of 128" (https://www.aqt.eu/aqt-pushing-performance-with-a-quantum-volume-of-128/). *AQT | ALPINE QUANTUM TECHNOLOGIES*. Retrieved February 13, 2023.
379. Bartolucci, Sara; Birchall, Patrick; Bombín, Hector; Cable, Hugo; Dawson, Chris; Gimeno-Segovia, Mercedes; Johnston, Eric; Kieling, Konrad; Nickerson, Naomi; Pant, Mihir; Pastawski, Fernando; Rudolph, Terry; Sparrow, Chris (February 17, 2023). "Fusion-based quantum computation" (https://www.nature.com/articles/s41467-023-36493-1). *Nature Communications*. **14** (1). doi:10.1038/s41467-023-36493-1 (https://doi.org/10.1038%2Fs41467-023-36493-1). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 9938229 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9938229). PMID 36805650 (https://pubmed.ncbi.nlm.nih.gov/36805650).

380. "India's first quantum computing-based telecom network link now operational: Ashwini Vaishnaw" (https://economictimes.indiatimes.com/industry/telecom/telecom-news/indias-first-quantum-computing-based-telecom-network-link-now-operational-ashwini-vaishnaw/articleshow/99026697.cms). *The Economic Times*. March 27, 2023.
381. Chang, Kenneth (June 14, 2023). "Quantum Computing Advance Begins New Era, IBM Says – A quantum computer came up with better answers to a physics problem than a conventional supercomputer" (https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html). *The New York Times*. Archived (https://archive.today/20230614151835/https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html) from the original on June 14, 2023. Retrieved June 15, 2023.
382. Kim, Youngseok; et al. (June 14, 2023). "Evidence for the utility of quantum computing before fault tolerance" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10266970). *Nature*. **618** (7965): 500–505. Bibcode:2023Natur.618..500K (https://ui.adsabs.harvard.edu/abs/2023Natur.618..500K). doi:10.1038/s41586-023-06096-3 (https://doi.org/10.1038%2Fs41586-023-06096-3). PMC 10266970 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10266970). PMID 37316724 (https://pubmed.ncbi.nlm.nih.gov/37316724).
383. Lardinois, Frederic (June 21, 2023). "Microsoft expects to build a quantum supercomputer within 10 years" (https://techcrunch.com/2023/06/21/microsoft-expects-to-build-a-quantum-supercomputer-within-10-years/?guccounter=1&guce_referrer=aHR0cHM6Ly9lZGdlOS5od3VwZ3JhZGUuaXQv&guce_referrer_sig=AQAAACXAB0qvUPp2WTkuGfdLz7J6WL84C0dFSnA7-JlfcbG-NlUc5Wr_rDCfeBFqRnEGLozBpwYqrxqWUim6CgPzx5HnmrvLTOgBuO9C3fptgIUZ2JvHF1205F6FgMmcC-qSSHXDFx_aNts3TXoSyHy7ovW9ixtgT47y8ID7RHz8bMUj). Tech Crunch.
384. Bluvstein, Dolev; Evered, Simon J.; Geim, Alexandra A.; Li, Sophie H.; Zhou, Hengyun; Manovitz, Tom; Ebadi, Sepehr; Cain, Madelyn; Kalinowski, Marcin; Hangleiter, Dominik; Bonilla Ataides, J. Pablo; Maskara, Nishad; Cong, Iris; Gao, Xun; Sales Rodriguez, Pedro; Karolyshyn, Thomas; Semeghini, Giulia; Gullans, Michael J.; Greiner, Markus; Vuletić, Vladan; Lukin, Mikhail D. (2024). "Logical quantum processor based on reconfigurable atom arrays" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). *Nature*. **626** (7997): 58–65. arXiv:2312.03982 (https://arxiv.org/abs/2312.03982). Bibcode:2024Natur.626...58B (https://ui.adsabs.harvard.edu/abs/2024Natur.626...58B). doi:10.1038/s41586-023-06927-3 (https://doi.org/10.1038%2Fs41586-023-06927-3). PMC 10830422 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). PMID 38056497 (https://pubmed.ncbi.nlm.nih.gov/38056497).
385. Pause, L.; Sturm, L.; Mittenbühler, M.; Amann, S.; Preuschoff, T.; Schäffner, D.; Schlosser, S.; Birkl, G. (2024). "Supercharged two-dimensional tweezer array with more than 1000 atomic qubits" (https://opg.optica.org/optica/abstract.cfm?URI=optica-11-2-222). *Optica*. **11** (2): 222–226. arXiv:2310.09191 (https://arxiv.org/abs/2310.09191). Bibcode:2024Optic..11..222P (https://ui.adsabs.harvard.edu/abs/2024Optic..11..222P). doi:10.1364/OPTICA.513551 (https://doi.org/10.1364%2FOPTICA.513551).
386. Dumke, R.; Volk, M.; Müther, T.; Buchkremer, F. B. J.; Birkl, G.; Ertmer, W. (August 8, 2002). "Micro-optical Realization of Arrays of Selectively Addressable Dipole Traps: A Scalable Configuration for Quantum Computation with Atomic Qubits" (https://link.aps.org/doi/10.1103/PhysRevLett.89.097903). *Physical Review Letters*. **89** (9): 097903. arXiv:quant-ph/0110140 (https://arxiv.org/abs/quant-ph/0110140). Bibcode:2002PhRvL..89i7903D (https://ui.adsabs.harvard.edu/abs/2002PhRvL..89i7903D). doi:10.1103/PhysRevLett.89.097903 (https://doi.org/10.1103%2FPhysRevLett.89.097903). PMID 12190441 (https://pubmed.ncbi.nlm.nih.gov/12190441).
387. "Quantum startup Atom Computing first to exceed 1,000 qubits" (https://atom-computing.com/quantum-startup-atom-computing-first-to-exceed-1000-qubits/). Boulder, CO. October 24, 2023.
388. Russell, John (October 24, 2023). "Atom Computing Wins the Race to 1000 Qubits" (https://www.hpcwire.com/2023/10/24/atom-computing-wins-the-race-to-1000-qubits/). HPC Wire.

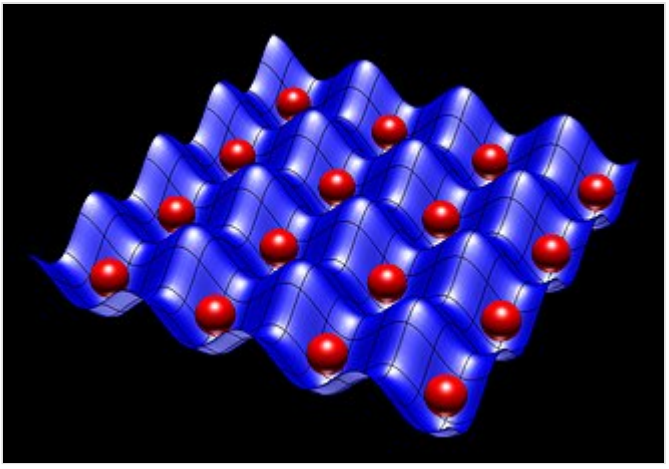
389. McDowell, Steve. "IBM Advances Quantum Computing with New Processors & Platforms" (https://www.forbes.com/sites/stevemcdowell/2023/12/05/ibm-advances-quantum-computing-with-new-processors--platforms/). *Forbes*. Retrieved December 27, 2023.
390. "IBM Quantum Computing Blog | The hardware and software for the era of quantum utility is here" (https://www.ibm.com/quantum/blog/quantum-roadmap-2033). *www.ibm.com*. Retrieved December 27, 2023.
391. "IBM's roadmap for scaling quantum technology" (https://research.ibm.com/blog/ibm-quantum-roadmap). *IBM Research Blog*. February 9, 2021. Retrieved December 27, 2023.
392. Bluvstein, Dolev; Evered, Simon J.; Geim, Alexandra A.; Li, Sophie H.; Zhou, Hengyun; Manovitz, Tom; Ebadi, Sepehr; Cain, Madelyn; Kalinowski, Marcin; Hangleiter, Dominik; Bonilla Ataides, J. Pablo; Maskara, Nishad; Cong, Iris; Gao, Xun; Sales Rodriguez, Pedro; Karolyshyn, Thomas; Semeghini, Giulia; Gullans, Michael J.; Greiner, Markus; Vuletić, Vladan; Lukin, Mikhail D. (2024). "Logical quantum processor based on reconfigurable atom arrays" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). *Nature*. **626** (7997): 58–65. arXiv:2312.03982 (https://arxiv.org/abs/2312.03982). Bibcode:2024Natur.626...58B (https://ui.adsabs.harvard.edu/abs/2024Natur.626...58B). doi:10.1038/s41586-023-06927-3 (https://doi.org/10.1038%2Fs41586-023-06927-3). PMC 10830422 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). PMID 38056497 (https://pubmed.ncbi.nlm.nih.gov/38056497).
393. Thomas, Philip; Ruscio, Leonardo; Morin, Olivier; Rempe, Gerhard (May 16, 2024). "Fusion of deterministically generated photonic graph states" (https://www.nature.com/articles/s41586-024-07357-5). *Nature*. **629** (8012): 567–572. doi:10.1038/s41586-024-07357-5 (https://doi.org/10.1038%2Fs41586-024-07357-5). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMC 11096110 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11096110). PMID 38720079 (https://pubmed.ncbi.nlm.nih.gov/38720079).
394. [hhttps://quantumcomputingreport.com/photonic-inc-demonstrates-distributed-entanglement-between-two-modules-separated-by-40-meters-of-fiber/ "Photonic Inc. Demonstrates Distributed Entanglement Between Two Modules Separated by 40 Meters of Fiber"]. *www.quantumcomputingreport.com*. May 30, 2024. Retrieved September 3, 2024.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Timeline_of_quantum_computing_and_communication&oldid=1243933877"

WIKIPEDIA
The Free Encyclopedia

Quantum information

Quantum information is the information of the state of a quantum system. It is the basic entity of study in **quantum information theory**,[1][2][3] and can be manipulated using quantum information processing techniques. Quantum information refers to both the technical definition in terms of Von Neumann entropy and the general computational term.



Optical lattices use lasers to separate rubidium atoms (red) for use as information bits in neutral-atom quantum processors—prototype devices which designers are trying to develop into full-fledged quantum computers.

It is an interdisciplinary field that involves quantum mechanics, computer science, information theory, philosophy and cryptography among other fields.[4][5][6] Its study is also relevant to disciplines such as cognitive science, psychology and neuroscience.[7][8][9][10] Its main focus is in extracting information from matter at the microscopic scale. Observation in science is one of the most important ways of acquiring information and measurement is required in order to quantify the observation, making this crucial to the scientific method. In quantum mechanics, due to the uncertainty principle, non-commuting observables cannot be precisely measured simultaneously, as an eigenstate in one basis is not an eigenstate in the other basis. According to the eigenstate–eigenvalue link, an observable is well-defined (definite) when the state of the system is an eigenstate of the observable.[11] Since any two non-commuting observables are not simultaneously well-defined, a quantum state can never contain definitive information about both non-commuting observables.[8]

Information is something physical that is encoded in the state of a quantum system.[12] While quantum mechanics deals with examining properties of matter at the microscopic level,[13][8] quantum information science focuses on extracting information from those properties,[8] and quantum computation manipulates and processes information – performs logical operations – using quantum information processing techniques.[14]

Quantum information, like classical information, can be processed using digital computers, transmitted from one location to another, manipulated with algorithms, and analyzed with computer science and mathematics. Just like the basic unit of classical information is the bit, quantum information deals with qubits.[15] Quantum information can be measured using Von Neumann entropy.

Recently, the field of quantum computing has become an active research area because of the possibility to disrupt modern computation, communication, and cryptography.[14][16]

History and development

Development from fundamental quantum mechanics

The history of quantum information theory began at the turn of the 20th century when classical physics was revolutionized into quantum physics. The theories of classical physics were predicting absurdities such as the ultraviolet catastrophe, or electrons spiraling into the nucleus. At first these problems were brushed aside by adding ad hoc hypotheses to classical physics. Soon, it became apparent that a new theory must be created in order to make sense of these absurdities, and the theory of quantum mechanics was born.[2]

Quantum mechanics was formulated by Schrödinger using wave mechanics and Heisenberg using matrix mechanics.[17] The equivalence of these methods was proven later.[18] Their formulations described the dynamics of microscopic systems but had several unsatisfactory aspects in describing measurement processes. Von Neumann formulated quantum theory using operator algebra in a way that it described measurement as well as dynamics.[19] These studies emphasized the philosophical aspects of measurement rather than a quantitative approach to extracting information via measurements.

See: Dynamical Pictures

Evolution of:	Picture ()		
	Schrödinger (S)	Heisenberg (H)	Interaction (I)
Ket state	$\vert\psi_\mathrm{S}(t)\rangle = e^{-iH_\mathrm{S}\ t/\hbar}\vert\psi_\mathrm{S}(0)\rangle$	constant	$\vert\psi_\mathrm{I}(t)\rangle = e^{iH_{0,\mathrm{S}}\ t/\hbar}\vert\psi_\mathrm{S}(t)\rangle$
Observable	constant	$A_\mathrm{H}(t) = e^{iH_\mathrm{S}\ t/\hbar}A_\mathrm{S}e^{-iH_\mathrm{S}\ t/\hbar}$	$A_\mathrm{I}(t) = e^{iH_{0,\mathrm{S}}\ t/\hbar}A_\mathrm{S}e^{-iH_{0,\mathrm{S}}\ t/\hbar}$
Density matrix	$\rho_\mathrm{S}(t) = e^{-iH_\mathrm{S}\ t/\hbar}\rho_\mathrm{S}(0)e^{iH_\mathrm{S}\ t/\hbar}$	constant	$\rho_\mathrm{I}(t) = e^{iH_{0,\mathrm{S}}\ t/\hbar}\rho_\mathrm{S}(t)e^{-iH_{0,\mathrm{S}}\ t/\hbar}$

Development from communication

In 1960s, Stratonovich, Helstrom and Gordon[20] proposed a formulation of optical communications using quantum mechanics. This was the first historical appearance of quantum information theory. They mainly studied error probabilities and channel capacities for communication.[20][21][22] Later, Alexander Holevo obtained an upper bound of communication speed in the transmission of a classical message via a quantum channel.[23][24]

Development from atomic physics and relativity

In the 1970s, techniques for manipulating single-atom quantum states, such as the atom trap and the scanning tunneling microscope, began to be developed, making it possible to isolate single atoms and arrange them in arrays. Prior to these developments, precise control over single quantum systems was not

possible, and experiments utilized coarser, simultaneous control over a large number of quantum systems.[2] The development of viable single-state manipulation techniques led to increased interest in the field of quantum information and computation.

In the 1980s, interest arose in whether it might be possible to use quantum effects to disprove Einstein's theory of relativity. If it were possible to clone an unknown quantum state, it would be possible to use entangled quantum states to transmit information faster than the speed of light, disproving Einstein's theory. However, the no-cloning theorem showed that such cloning is impossible. The theorem was one of the earliest results of quantum information theory.[2]

Development from cryptography

Despite all the excitement and interest over studying isolated quantum systems and trying to find a way to circumvent the theory of relativity, research in quantum information theory became stagnant in the 1980s. However, around the same time another avenue started dabbling into quantum information and computation: Cryptography. In a general sense, *cryptography is the problem of doing communication or computation involving two or more parties who may not trust one another.*[2]

Bennett and Brassard developed a communication channel on which it is impossible to eavesdrop without being detected, a way of communicating secretly at long distances using the BB84 quantum cryptographic protocol.[25] The key idea was the use of the fundamental principle of quantum mechanics that observation disturbs the observed, and the introduction of an eavesdropper in a secure communication line will immediately let the two parties trying to communicate know of the presence of the eavesdropper.

Development from computer science and mathematics

With the advent of Alan Turing's revolutionary ideas of a programmable computer, or Turing machine, he showed that any real-world computation can be translated into an equivalent computation involving a Turing machine.[26][27] This is known as the Church–Turing thesis.

Soon enough, the first computers were made, and computer hardware grew at such a fast pace that the growth, through experience in production, was codified into an empirical relationship called Moore's law. This 'law' is a projective trend that states that the number of transistors in an integrated circuit doubles every two years.[28] As transistors began to become smaller and smaller in order to pack more power per surface area, quantum effects started to show up in the electronics resulting in inadvertent interference. This led to the advent of quantum computing, which used quantum mechanics to design algorithms.

At this point, quantum computers showed promise of being much faster than classical computers for certain specific problems. One such example problem was developed by David Deutsch and Richard Jozsa, known as the Deutsch–Jozsa algorithm. This problem however held little to no practical applications.[2] Peter Shor in 1994 came up with a very important and practical problem, one of finding the prime factors of an integer. The discrete logarithm problem as it was called, could be solved efficiently on a quantum computer but not on a classical computer hence showing that quantum computers are more powerful than Turing machines.

Development from information theory

Around the time computer science was making a revolution, so was information theory and communication, through Claude Shannon.[29][30][31] Shannon developed two fundamental theorems of information theory: noiseless channel coding theorem and noisy channel coding theorem. He also showed that error correcting codes could be used to protect information being sent.

Quantum information theory also followed a similar trajectory, Ben Schumacher in 1995 made an analogue to Shannon's noiseless coding theorem using the qubit. A theory of error-correction also developed, which allows quantum computers to make efficient computations regardless of noise and make reliable communication over noisy quantum channels.[2]

Qubits and information theory

Quantum information differs strongly from classical information, epitomized by the bit, in many striking and unfamiliar ways. While the fundamental unit of classical information is the bit, the most basic unit of quantum information is the qubit. Classical information is measured using Shannon entropy, while the quantum mechanical analogue is Von Neumann entropy. Given a statistical ensemble of quantum mechanical systems with the density matrix ρ, it is given by $S(\rho) = -\operatorname{Tr}(\rho \ln \rho)$.[2] Many of the same entropy measures in classical information theory can also be generalized to the quantum case, such as Holevo entropy[32] and the conditional quantum entropy.

Unlike classical digital states (which are discrete), a qubit is continuous-valued, describable by a direction on the Bloch sphere. Despite being continuously valued in this way, a qubit is the *smallest* possible unit of quantum information, and despite the qubit state being continuous-valued, it is impossible to measure the value precisely. Five famous theorems describe the limits on manipulation of quantum information.[2]

1. no-teleportation theorem, which states that a qubit cannot be (wholly) converted into classical bits; that is, it cannot be fully "read".
2. no-cloning theorem, which prevents an arbitrary qubit from being copied.
3. no-deleting theorem, which prevents an arbitrary qubit from being deleted.
4. no-broadcast theorem, which prevents an arbitrary qubit from being delivered to multiple recipients, although it can be transported from place to place (*e.g.* via quantum teleportation).
5. no-hiding theorem, which demonstrates the conservation of quantum information.

These theorems are proven from unitarity, which according to Leonard Susskind is the technical term for the statement that quantum information within the universe is conserved.[33]:94 The five theorems open up possibilities in quantum information processing.

Quantum information processing

The state of a qubit contains all of its information. This state is frequently expressed as a vector on the Bloch sphere. This state can be changed by applying linear transformations or quantum gates to them. These unitary transformations are described as rotations on the Bloch Sphere. While classical gates correspond to the familiar operations of Boolean logic, quantum gates are physical unitary operators.

- Due to the volatility of quantum systems and the impossibility of copying states, the storing of quantum information is much more difficult than storing classical information.

Nevertheless, with the use of quantum error correction quantum information can still be reliably stored in principle. The existence of quantum error correcting codes has also led to the possibility of fault-tolerant quantum computation.

- Classical bits can be encoded into and subsequently retrieved from configurations of qubits, through the use of quantum gates. By itself, a single qubit can convey no more than one bit of accessible classical information about its preparation. This is Holevo's theorem. However, in superdense coding a sender, by acting on one of two entangled qubits, can convey two bits of accessible information about their joint state to a receiver.
- Quantum information can be moved about, in a quantum channel, analogous to the concept of a classical communications channel. Quantum messages have a finite size, measured in qubits; quantum channels have a finite channel capacity, measured in qubits per second.
- Quantum information, and changes in quantum information, can be quantitatively measured by using an analogue of Shannon entropy, called the von Neumann entropy.
- In some cases, quantum algorithms can be used to perform computations faster than in any known classical algorithm. The most famous example of this is Shor's algorithm that can factor numbers in polynomial time, compared to the best classical algorithms that take sub-exponential time. As factorization is an important part of the safety of RSA encryption, Shor's algorithm sparked the new field of post-quantum cryptography that tries to find encryption schemes that remain safe even when quantum computers are in play. Other examples of algorithms that demonstrate quantum supremacy include Grover's search algorithm, where the quantum algorithm gives a quadratic speed-up over the best possible classical algorithm. The complexity class of problems efficiently solvable by a quantum computer is known as BQP.
- Quantum key distribution (QKD) allows unconditionally secure transmission of classical information, unlike classical encryption, which can always be broken in principle, if not in practice. Do note that certain subtle points regarding the safety of QKD are still hotly debated.

The study of all of the above topics and differences comprises quantum information theory.

Relation to quantum mechanics

Quantum mechanics is the study of how microscopic physical systems change dynamically in nature. In the field of quantum information theory, the quantum systems studied are abstracted away from any real world counterpart. A qubit might for instance physically be a photon in a linear optical quantum computer, an ion in a trapped ion quantum computer, or it might be a large collection of atoms as in a superconducting quantum computer. Regardless of the physical implementation, the limits and features of qubits implied by quantum information theory hold as all these systems are mathematically described by the same apparatus of density matrices over the complex numbers. Another important difference with quantum mechanics is that while quantum mechanics often studies infinite-dimensional systems such as a harmonic oscillator, quantum information theory is concerned with both continuous-variable systems[34] and finite-dimensional systems.[8][35][36]

Entropy and information

Entropy measures the uncertainty in the state of a physical system.[2] Entropy can be studied from the point of view of both the classical and quantum information theories.

Classical information theory

Classical information is based on the concepts of information laid out by Claude Shannon. Classical information, in principle, can be stored in a bit of binary strings. Any system having two states is a capable bit.[37]

Shannon entropy

Shannon entropy is the quantification of the information gained by measuring the value of a random variable. Another way of thinking about it is by looking at the uncertainty of a system prior to measurement. As a result, entropy, as pictured by Shannon, can be seen either as a measure of the uncertainty prior to making a measurement or as a measure of information gained after making said measurement.[2]

Shannon entropy, written as a functional of a discrete probability distribution, $P(x_1), P(x_2), \ldots, P(x_n)$ associated with events $x_1, \ldots, x_n$, can be seen as the average information associated with this set of events, in units of bits:

$$H(X) = H[P(x_1), P(x_2), \ldots, P(x_n)] = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i)$$

This definition of entropy can be used to quantify the physical resources required to store the output of an information source. The ways of interpreting Shannon entropy discussed above are usually only meaningful when the number of samples of an experiment is large.[35]

Rényi entropy

The Rényi entropy is a generalization of Shannon entropy defined above. The Rényi entropy of order r, written as a function of a discrete probability distribution, $P(a_1), P(a_2), \ldots, P(a_n)$, associated with events $a_1, \ldots, a_n$, is defined as:[37]

$$H_r(A) = \frac{1}{1-r} \log_2 \sum_{i=1}^{n} P^r(a_i)$$

for $0 < r < \infty$ and $r \neq 1$.

We arrive at the definition of Shannon entropy from Rényi when $r \to 1$, of Hartley entropy (or max-entropy) when $r \to 0$, and min-entropy when $r \to \infty$.

Quantum information theory

Quantum information theory is largely an extension of classical information theory to quantum systems. Classical information is produced when measurements of quantum systems are made.[37]

Von Neumann entropy

One interpretation of Shannon entropy was the uncertainty associated with a probability distribution. When we want to describe the information or the uncertainty of a quantum state, the probability distributions are simply replaced by density operators ρ:

$$S(\rho) \equiv -\mathrm{tr}(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i,$$

where λ_i are the eigenvalues of ρ.

Von Neumann entropy plays a role in quantum information similar to the role Shannon entropy plays in classical information.

Applications

Quantum communication

Quantum communication is one of the applications of quantum physics and quantum information. There are some famous theorems such as the no-cloning theorem that illustrate some important properties in quantum communication. Dense coding and quantum teleportation are also applications of quantum communication. They are two opposite ways to communicate using qubits. While teleportation transfers one qubit from Alice and Bob by communicating two classical bits under the assumption that Alice and Bob have a pre-shared Bell state, dense coding transfers two classical bits from Alice to Bob by using one qubit, again under the same assumption, that Alice and Bob have a pre-shared Bell state.

Quantum key distribution

One of the best known applications of quantum cryptography is quantum key distribution which provide a theoretical solution to the security issue of a classical key. The advantage of quantum key distribution is that it is impossible to copy a quantum key because of the no-cloning theorem. If someone tries to read encoded data, the quantum state being transmitted will change. This could be used to detect eavesdropping.

BB84

The first quantum key distribution scheme, BB84, was developed by Charles Bennett and Gilles Brassard in 1984. It is usually explained as a method of securely communicating a private key from a third party to another for use in one-time pad encryption.[2]

E91

E91 was made by Artur Ekert in 1991. His scheme uses entangled pairs of photons. These two photons can be created by Alice, Bob, or by a third party including eavesdropper Eve. One of the photons is distributed to Alice and the other to Bob so that each one ends up with one photon from the pair.

This scheme relies on two properties of quantum entanglement:

1. The entangled states are perfectly correlated which means that if Alice and Bob both measure their particles having either a vertical or horizontal polarization, they always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. This necessitates that the two distant parties have exact directionality synchronization. However, from quantum mechanics theory the quantum state is completely random so that it is impossible for Alice to predict if she will get vertical polarization or horizontal polarization results.
2. Any attempt at eavesdropping by Eve destroys this quantum entanglement such that Alice and Bob can detect.

B92

B92 is a simpler version of BB84.[38]

The main difference between B92 and BB84:

- B92 only needs two states
- BB84 needs 4 polarization states

Like the BB84, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses the bases she must use. Bob still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything which is guaranteed by quantum mechanics theories. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly.[39]

Quantum computation

The most widely used model in quantum computation is the quantum circuit, which are based on the quantum bit "qubit". Qubit is somewhat analogous to the bit in classical computation. Qubits can be in a 1 or 0 quantum state, or they can be in a superposition of the 1 and 0 states. However, when qubits are measured the result of the measurement is always either a 0 or a 1; the probabilities of these two outcomes depend on the quantum state that the qubits were in immediately prior to the measurement.

Any quantum computation algorithm can be represented as a network of quantum logic gates.

Quantum decoherence

If a quantum system were perfectly isolated, it would maintain coherence perfectly, but it would be impossible to test the entire system. If it is not perfectly isolated, for example during a measurement, coherence is shared with the environment and appears to be lost with time; this process is called quantum decoherence. As a result of this process, quantum behavior is apparently lost, just as energy appears to be lost by friction in classical mechanics.

Quantum error correction

QEC is used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction is essential if one is to achieve fault-tolerant quantum computation that can deal not only with noise on stored quantum information, but also with faulty quantum gates, faulty quantum preparation, and faulty measurements.

Peter Shor first discovered this method of formulating a *quantum error correcting code* by storing the information of one qubit onto a highly entangled state of ancilla qubits. A quantum error correcting code protects quantum information against errors.

Journals

Many journals publish research in quantum information science, although only a few are dedicated to this area. Among these are:

- *International Journal of Quantum Information*
- *npj Quantum Information*
- *Quantum*
- *Quantum Information & Computation (https://www.rintonpress.com/journals/qic/)*
- *Quantum Information Processing (https://www.springer.com/journal/11128)*

- *Quantum Science and Technology (https://iopscience.iop.org/journal/2058-9565)*

See also

- Categorical quantum mechanics
- Einstein's thought experiments
- Interpretations of quantum mechanics
- Positive Operator Valued Measure (POVM)
- Quantum clock
- Quantum entanglement
- Quantum foundations
- Quantum information science
- Quantum statistical mechanics
- Qubit
- Qutrit
- Typical subspace

References

1. Vedral, Vlatko (2006). *Introduction to Quantum Information Science*. Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780199215706.001.0001 (https://doi.org/10.1093%2Facprof%3Aoso%2F9780199215706.001.0001). ISBN 9780199215706. OCLC 822959053 (https://search.worldcat.org/oclc/822959053).
2. Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information* (10th anniversary ed.). Cambridge: Cambridge University Press. doi:10.1017/cbo9780511976667 (https://doi.org/10.1017%2Fcbo9780511976667). ISBN 9780511976667. OCLC 665137861 (https://search.worldcat.org/oclc/665137861). S2CID 59717455 (https://api.semanticscholar.org/CorpusID:59717455).
3. Hayashi, Masahito (2006). *Quantum Information: An Introduction*. Berlin: Springer. doi:10.1007/3-540-30266-2 (https://doi.org/10.1007%2F3-540-30266-2). ISBN 978-3-540-30266-7. OCLC 68629072 (https://search.worldcat.org/oclc/68629072).
4. Bokulich, Alisa; Jaeger, Gregg (2010). *Philosophy of Quantum Information and Entanglement* (https://books.google.com/books?id=ZC_XB7MLcC8C). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511676550 (https://doi.org/10.1017%2FCBO9780511676550). ISBN 9780511676550.
5. Benatti, Fabio; Fannes, Mark; Floreanini, Roberto; Petritis, Dimitri (2010). *Quantum Information, Computation and Cryptography: An Introductory Survey of Theory, Technology and Experiments* (https://books.google.com/books?id=_0A8Qf1DYIgC). Lecture Notes in Physics. Vol. 808. Berlin: Springer. doi:10.1007/978-3-642-11914-9 (https://doi.org/10.1007%2F978-3-642-11914-9). ISBN 978-3-642-11914-9.
6. Benatti, Fabio (2009). "Quantum Information Theory". *Quantum Entropies*. Theoretical and Mathematical Physics. Dordrecht: Springer. pp. 255–315. doi:10.1007/978-1-4020-9306-7_6 (https://doi.org/10.1007%2F978-1-4020-9306-7_6). ISBN 978-1-4020-9306-7.
7. Hayashi, Masahito; Ishizaka, Satoshi; Kawachi, Akinori; Kimura, Gen; Ogawa, Tomohiro (2015). *Introduction to Quantum Information Science*. Berlin: Springer. Bibcode:2015iqis.book.....H (https://ui.adsabs.harvard.edu/abs/2015iqis.book.....H). doi:10.1007/978-3-662-43502-1 (https://doi.org/10.1007%2F978-3-662-43502-1). ISBN 978-3-662-43502-1.

8. Hayashi, Masahito (2017). *Quantum Information Theory: Mathematical Foundation*. Graduate Texts in Physics. Berlin: Springer. doi:10.1007/978-3-662-49725-8 (https://doi.org/10.1007%2F978-3-662-49725-8). ISBN 978-3-662-49725-8.
9. Georgiev, Danko D. (2017-12-06). *Quantum Information and Consciousness: A Gentle Introduction* (https://books.google.com/books?id=OtRBDwAAQBAJ). Boca Raton: CRC Press. doi:10.1201/9780203732519 (https://doi.org/10.1201%2F9780203732519). ISBN 9781138104488. OCLC 1003273264 (https://search.worldcat.org/oclc/1003273264). Zbl 1390.81001 (https://zbmath.org/?format=complete&q=an:1390.81001).
10. Georgiev, Danko D. (2020). "Quantum information theoretic approach to the mind-brain problem". *Progress in Biophysics and Molecular Biology*. **158**: 16–32. arXiv:2012.07836 (https://arxiv.org/abs/2012.07836). doi:10.1016/j.pbiomolbio.2020.08.002 (https://doi.org/10.1016%2Fj.pbiomolbio.2020.08.002). PMID 32822698 (https://pubmed.ncbi.nlm.nih.gov/32822698). S2CID 221237249 (https://api.semanticscholar.org/CorpusID:221237249).
11. Gilton, Marian J. R. (2016). "Whence the eigenstate–eigenvalue link?". *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*. **55**: 92–100. Bibcode:2016SHPMP..55...92G (https://ui.adsabs.harvard.edu/abs/2016SHPMP..55...92G). doi:10.1016/j.shpsb.2016.08.005 (https://doi.org/10.1016%2Fj.shpsb.2016.08.005).
12. Preskill, John. *Quantum Computation (Physics 219/Computer Science 219)* (http://www.theory.caltech.edu/~preskill/ph219/). Pasadena, California: California Institute of Technology.
13. Feynman, Richard Phillips; Leighton, Robert Benjamin; Sands, Matthew Linzee (2013). "Quantum behavior". *The Feynman Lectures on Physics. Volume III. Quantum Mechanics* (https://www.feynmanlectures.caltech.edu/III_01.html). Pasadena, California: California Institute of Technology.
14. Lo, Hoi-Kwong; Popescu, Sandu; Spiller, Tim (1998). *Introduction to Quantum Computation and Information* (https://books.google.com/books?id=18_-rgkdQGIC). Singapore: World Scientific. Bibcode:1998iqci.book.....S (https://ui.adsabs.harvard.edu/abs/1998iqci.book.....S). doi:10.1142/3724 (https://doi.org/10.1142%2F3724). ISBN 978-981-4496-35-3. OCLC 52859247 (https://search.worldcat.org/oclc/52859247).
15. Bennett, Charles H.; Shor, Peter Williston (1998). "Quantum information theory". *IEEE Transactions on Information Theory*. **44** (6): 2724–2742. CiteSeerX 10.1.1.89.1572 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.89.1572). doi:10.1109/18.720553 (https://doi.org/10.1109%2F18.720553).
16. Garlinghouse, Tom (2020). "Quantum computing: Opening new realms of possibilities" (https://www.princeton.edu/news/2020/01/21/quantum-computing-opening-new-realms-possibilities). *Discovery: Research at Princeton*: 12–17.
17. Mahan, Gerald D. (2009). *Quantum Mechanics in a Nutshell*. Princeton: Princeton University Press. doi:10.2307/j.ctt7s8nw (https://doi.org/10.2307%2Fj.ctt7s8nw). ISBN 978-1-4008-3338-2. JSTOR j.ctt7s8nw (https://www.jstor.org/stable/j.ctt7s8nw).
18. Perlman, H. S. (1964). "Equivalence of the Schroedinger and Heisenberg pictures". *Nature*. **204** (4960): 771–772. Bibcode:1964Natur.204..771P (https://ui.adsabs.harvard.edu/abs/1964Natur.204..771P). doi:10.1038/204771b0 (https://doi.org/10.1038%2F204771b0). S2CID 4194913 (https://api.semanticscholar.org/CorpusID:4194913).
19. Neumann, John von (2018-02-27). *Mathematical Foundations of Quantum Mechanics: New Edition* (https://books.google.com/books?id=B3OYDwAAQBAJ&q=foundations+of+quantum+mechanics+von+neumann&pg=PR1). Princeton University Press. ISBN 978-0-691-17856-1.
20. Gordon, J. P. (1962). "Quantum effects in communications systems". *Proceedings of the IRE*. **50** (9): 1898–1908. doi:10.1109/jrproc.1962.288169 (https://doi.org/10.1109%2Fjrproc.1962.288169). S2CID 51631629 (https://api.semanticscholar.org/CorpusID:51631629).

21. Helstrom, Carl W. (1969). "Quantum detection and estimation theory". *Journal of Statistical Physics*. **1** (2): 231–252. Bibcode:1969JSP.....1..231H (https://ui.adsabs.harvard.edu/abs/1969JSP.....1..231H). doi:10.1007/bf01007479 (https://doi.org/10.1007%2Fbf01007479). hdl:2060/19690016211 (https://hdl.handle.net/2060%2F19690016211). S2CID 121571330 (https://api.semanticscholar.org/CorpusID:121571330).
22. Helstrom, Carl W. (1976). *Quantum Detection and Estimation Theory*. Mathematics in Science and Engineering. Vol. 123. New York: Academic Press. doi:10.1016/s0076-5392(08)x6017-5 (https://doi.org/10.1016%2Fs0076-5392%2808%29x6017-5). hdl:2060/19690016211 (https://hdl.handle.net/2060%2F19690016211). ISBN 9780080956329. OCLC 2020051 (https://search.worldcat.org/oclc/2020051).
23. Holevo, Alexander S. (1973). "Bounds for the quantity of information transmitted by a quantum communication channel" (https://mi.mathnet.ru/ppi903). *Problems of Information Transmission*. **9** (3): 177–183. MR 0456936 (https://mathscinet.ams.org/mathscinet-getitem?mr=0456936). Zbl 0317.94003 (https://zbmath.org/?format=complete&q=an:0317.94003).
24. Holevo, Alexander S. (1979). "On capacity of a quantum communications channel" (https://mi.mathnet.ru/ppi1507). *Problems of Information Transmission*. **15** (4): 247–253. MR 0581651 (https://mathscinet.ams.org/mathscinet-getitem?mr=0581651). Zbl 0433.94008 (https://zbmath.org/?format=complete&q=an:0433.94008).
25. Bennett, Charles H.; Brassard, Gilles (2014). "Quantum cryptography: public key distribution and coin tossing". *Theoretical Computer Science*. **560** (1): 7–11. arXiv:2003.06557 (https://arxiv.org/abs/2003.06557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025). S2CID 27022972 (https://api.semanticscholar.org/CorpusID:27022972).
26. Weisstein, Eric W. "Church–Turing Thesis" (https://mathworld.wolfram.com/Church-TuringThesis.html). *mathworld.wolfram.com*. Retrieved 2020-11-13.
27. Deutsch, David (1985). "Quantum theory, the Church–Turing principle and the universal quantum computer". *Proceedings of the Royal Society of London A: Mathematical and Physical Sciences*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D (https://ui.adsabs.harvard.edu/abs/1985RSPSA.400...97D). doi:10.1098/rspa.1985.0070 (https://doi.org/10.1098%2Frspa.1985.0070). S2CID 1438116 (https://api.semanticscholar.org/CorpusID:143811 6).
28. Moore, Gordon Earle (1998). "Cramming more components onto integrated circuits". *Proceedings of the IEEE*. **86** (1): 82–85. doi:10.1109/jproc.1998.658762 (https://doi.org/10.1109%2Fjproc.1998.658762). S2CID 6519532 (https://api.semanticscholar.org/CorpusID:6519532).
29. Shannon, Claude E. (1948). "A mathematical theory of communication". *The Bell System Technical Journal*. **27** (3): 379–423. doi:10.1002/j.1538-7305.1948.tb01338.x (https://doi.org/10.1002%2Fj.1538-7305.1948.tb01338.x).
30. Shannon, Claude E. (1948). "A mathematical theory of communication". *The Bell System Technical Journal*. **27** (4): 623–656. doi:10.1002/j.1538-7305.1948.tb00917.x (https://doi.org/10.1002%2Fj.1538-7305.1948.tb00917.x).
31. Shannon, Claude E.; Weaver, Warren (1964). *The Mathematical Theory of Communication* (http://hdl.handle.net/11858/00-001M-0000-002C-4314-2). Urbana: University of Illinois Press. hdl:11858/00-001M-0000-002C-4314-2 (https://hdl.handle.net/11858%2F00-001M-0000-002C-4314-2).
32. "Alexandr S. Holevo" (https://www.mi.ras.ru/~holevo/eindex.html). *Mi.ras.ru*. Retrieved 4 December 2018.
33. Susskind, Leonard; Friedman, Art (2014). *Quantum Mechanics: The Theoretical Minimum. What You Need to Know to Start Doing Physics* (https://books.google.com/books?id=iQE4DgAAQBAJ&pg=PT83). New York: Basic Books. ISBN 978-0-465-08061-8. OCLC 1038428525 (https://search.worldcat.org/oclc/1038428525).

34. Weedbrook, Christian; Pirandola, Stefano; García-Patrón, Raúl; Cerf, Nicolas J.; Ralph, Timothy C.; Shapiro, Jeffrey H.; Lloyd, Seth (2012). "Gaussian quantum information". *Reviews of Modern Physics*. **84** (2): 621–669. arXiv:1110.3234 (https://arxiv.org/abs/1110.3234). Bibcode:2012RvMP...84..621W (https://ui.adsabs.harvard.edu/abs/2012RvMP...84..621W). doi:10.1103/RevModPhys.84.621 (https://doi.org/10.1103%2FRevModPhys.84.621). S2CID 119250535 (https://api.semanticscholar.org/CorpusID:119250535).
35. Watrous, John (2018). *The Theory of Quantum Information* (https://cs.uwaterloo.ca/~watrous/TQI/). Cambridge: Cambridge University Press. doi:10.1017/9781316848142 (https://doi.org/10.1017%2F9781316848142). ISBN 9781316848142. OCLC 1034577167 (https://search.worldcat.org/oclc/1034577167).
36. Wilde, Mark M. (2017). *Quantum Information Theory* (2nd ed.). Cambridge: Cambridge University Press. arXiv:1106.1445 (https://arxiv.org/abs/1106.1445). doi:10.1017/9781316809976 (https://doi.org/10.1017%2F9781316809976). ISBN 9781316809976.
37. Jaeger, Gregg (2007). *Quantum Information: An Overview* (https://books.google.com/books?id=E0ho97k7S4oC). New York: Springer. doi:10.1007/978-0-387-36944-0 (https://doi.org/10.1007%2F978-0-387-36944-0). ISBN 978-0-387-36944-0. OCLC 255569451 (https://search.worldcat.org/oclc/255569451).
38. Bennett, Charles H. (1992). "Quantum cryptography using any two nonorthogonal states". *Physical Review Letters*. **68** (21): 3121–3124. Bibcode:1992PhRvL..68.3121B (https://ui.adsabs.harvard.edu/abs/1992PhRvL..68.3121B). doi:10.1103/PhysRevLett.68.3121 (https://doi.org/10.1103%2FPhysRevLett.68.3121). PMID 10045619 (https://pubmed.ncbi.nlm.nih.gov/10045619). S2CID 19708593 (https://api.semanticscholar.org/CorpusID:19708593).
39. Haitjema, Mart (2007). *A Survey of the Prominent Quantum Key Distribution Protocols* (https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/#b92). Washington University in St. Louis. S2CID 18346434 (https://api.semanticscholar.org/CorpusID:18346434).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_information&oldid=1223840276"

WIKIPEDIA
The Free Encyclopedia

Quantum programming

Quantum programming is the process of designing or assembling sequences of instructions, called quantum circuits, using gates, switches, and operators to manipulate a quantum system for a desired outcome or results of a given experiment. Quantum circuit algorithms can be implemented on integrated circuits, conducted with instrumentation, or written in a programming language for use with a quantum computer or a quantum processor.

With quantum processor based systems, quantum programming languages help express quantum algorithms using high-level constructs.[1] The field is deeply rooted in the open-source philosophy and as a result most of the quantum software discussed in this article is freely available as open-source software.[2]

Quantum computers, such as those based on the KLM protocol, a linear optical quantum computing (LOQC) model, use quantum algorithms (circuits) implemented with electronics, integrated circuits, instrumentation, sensors, and/or by other physical means.

Other circuits designed for experimentation related to quantum systems can be instrumentation and sensor based.

Quantum instruction sets

Quantum instruction sets are used to turn higher level algorithms into physical instructions that can be executed on quantum processors. Sometimes these instructions are specific to a given hardware platform, e.g. ion traps or superconducting qubits.

Blackbird

Blackbird[3][4] is a quantum instruction set and intermediate representation used by Xanadu Quantum Technologies and Strawberry Fields. It is designed to represent continuous-variable quantum programs that can run on photonic quantum hardware.

cQASM

cQASM,[5] also known as common QASM, is a hardware-agnostic quantum assembly language which guarantees the interoperability between all the quantum compilation and simulation tools. It was introduced by the QCA Lab at TUDelft.

OpenQASM

OpenQASM[6] is the intermediate representation introduced by IBM for use with Qiskit and the IBM Q Experience.

Quil

Quil is an instruction set architecture for quantum computing that first introduced a shared quantum/classical memory model. It was introduced by Robert Smith, Michael Curtis, and William Zeng in *A Practical Quantum Instruction Set Architecture*.[7] Many quantum algorithms (including quantum teleportation, quantum error correction, simulation,[8][9] and optimization algorithms[10]) require a shared memory architecture.

Quantum software development kits

Quantum software development kits provide collections of tools to create and manipulate quantum programs.[11] They also provide the means to simulate the quantum programs or prepare them to be run using cloud-based quantum devices and self-hosted quantum devices.

SDKs with access to quantum processors

The following software development kits can be used to run quantum circuits on prototype quantum devices, as well as on simulators.

Cirq

An open source project developed by Google, which uses the Python programming language to create and manipulate quantum circuits. Programs written in Cirq can be run on IonQ, Pasqal,[12] Rigetti, and Alpine Quantum Technologies.[13]

Classiq

A cloud-based quantum IDE developed by Classiq, uses a high-level quantum language, Qmod, to generate scalable and efficient quantum circuits with a hardware-aware synthesis engine, that can be deployed across a wide range of QPUs. The platform includes a large library of quantum algorithms.

Forest

An open source project developed by Rigetti, which uses the Python programming language to create and manipulate quantum circuits. Results are obtained either using simulators or prototype quantum devices provided by Rigetti. As well as the ability to create programs using basic quantum operations, higher level algorithms are available within the Grove package.[14] Forest is based on the Quil instruction set.

MindQuantum

MindQuantum is a quantum computing framework based on MindSpore, focusing on the implementation of NISQ algorithms.[15][16][17]

Ocean

An open source suite of tools developed by D-Wave. Written mostly in the Python programming language, it enables users to formulate problems in Ising Model and Quadratic Unconstrained Binary Optimization formats (QUBO). Results can be obtained by submitting to an online quantum computer in Leap, D-Wave's real-time Quantum Application Environment, customer-owned machines, or classical samplers.

PennyLane

An open-source Python library developed by Xanadu Quantum Technologies for differentiable programming of quantum computers.[18][19][20][21] PennyLane provides users the ability to create models using TensorFlow, NumPy, or PyTorch, and connect them with quantum computer backends available from IBMQ, Google Quantum, Rigetti, Quantinuum[22] and Alpine Quantum Technologies.[13][23]

```python
from projectq import MainEngine        # import the main compiler engine
from projectq.ops import H, Measure, X # import the operations we want to
                                       # perform (Hadamard, X, measurement)

eng = MainEngine()   # create a default compiler (the backend is a simulator)
qubit = eng.allocate_qubit() # allocate 1 qubit

H | qubit # apply a Hadamard gate
X | qubit # apply an X gate
Measure | qubit # measure the qubit

eng.flush() # flush all gates (and execute measurements)
print("Measured {}".format(int(qubit))) # output measurement result

#
# Output: "Measured 1"
#
# Note that this is the (slow) Python simulator.
```

A sample code using projectq with Python

Perceval

An open-source project created by Quandela for designing photonic quantum circuits and developing quantum algorithms, based on Python. Simulations are run either on the user's own computer or on the cloud. Perceval is also used to connect to Quandela's cloud-based photonic quantum processor.[24][25]

ProjectQ

An open source project developed at the Institute for Theoretical Physics at ETH, which uses the Python programming language to create and manipulate quantum circuits.[26] Results are obtained either using a simulator, or by sending jobs to IBM quantum devices.

Qibo

An open source full-stack API for quantum simulation, quantum hardware control and calibration developed by multiple research laboratories, including QRC, CQT and INFN. Qibo (https://github.com/qiboteam/qibo) is a modular framework which includes multiple backends for quantum simulation and hardware control.[27][28] This project aims at providing a platform agnostic quantum hardware control framework with drivers for multiple instruments[29] and tools for quantum calibration, characterization and validation.[30] This framework focuses on self-hosted quantum devices by simplifying the software development required in labs.

Qiskit

An open source project developed by IBM.[31] Quantum circuits are created and manipulated using Python. Results are obtained either using simulators that run on the user's own device, simulators provided by IBM or prototype quantum devices provided by IBM. As well as the ability to create

programs using basic quantum operations, higher level tools for algorithms and benchmarking are available within specialized packages.[32] Qiskit is based on the OpenQASM standard for representing quantum circuits. It also supports pulse level control of quantum systems via QiskitPulse standard.[33]

Qrisp

Qrisp[34] is an open source project coordinated by the Eclipse Foundation[35] and developed in Python programming by Fraunhofer FOKUS[36] Qrisp is a high-level programming language for creating and compiling quantum algorithms. Its structured programming model enables scalable development and maintenance. The expressive syntax is based on variables instead of qubits, with the QuantumVariable as core class, and functions instead of gates. Additional tools, such as a performant simulator and automatic uncomputation, complement the extensive framework. Furthermore, it is platform independent, since it offers alternative compilation of elementary functions down to the circuit level, based on device-specific gate sets.

Quantum Development Kit

A project developed by Microsoft[37] as part of the .NET Framework. Quantum programs can be written and run within Visual Studio and VSCode using the quantum programming language Q#. Programs developed in the QDK can be run on Microsoft's Azure Quantum,[38] and run on quantum computers from Quantinuum,[22] IonQ, and Pasqal.[12]

Strawberry Fields

An open-source Python library developed by Xanadu Quantum Technologies for designing, simulating, and optimizing continuous variable (CV) quantum optical circuits.[39][40] Three simulators are provided - one in the Fock basis, one using the Gaussian formulation of quantum optics,[41] and one using the TensorFlow machine learning library. Strawberry Fields is also the library for executing programs on Xanadu's quantum photonic hardware.[42][43]

t|ket>

A quantum programming environment and optimizing compiler developed by Cambridge Quantum Computing that targets simulators and several quantum hardware back-ends, released in December 2018.[44]

Quantum programming languages

There are two main groups of quantum programming languages: imperative quantum programming languages and functional quantum programming languages.

Imperative languages

The most prominent representatives of the imperative languages are QCL,[45] LanQ[46] and Q|SI>.[47]

Ket

Ket[48] is an open-source embedded language designed to facilitate quantum programming, leveraging the familiar syntax and simplicity of Python. It serves as an integral component of the Ket Quantum Programming Platform,[49] seamlessly integrating with a Rust runtime library and a quantum simulator. Maintained by Quantuloop, the project emphasizes accessibility and versatility for researchers and developers. The following example demonstrates the implementation of a Bell state using Ket:

```
from ket import *
a, b = quant(2) # Allocate two quantum bits
H(a) # Put qubit `a` in a superposition
cnot(a, b) # Entangle the two qubits in the Bell state
m_a = measure(a) # Measure qubit `a`, collapsing qubit `b` as well
m_b = measure(b) # Measure qubit `b`
# Assert that the measurement of both qubits will always be equal
assert m_a.value == m_b.value
```

LQP

The Logic of Quantum Programs (LQP) is a dynamic quantum logic, capable of expressing important features of quantum measurements and unitary evolutions of multi-partite states, and provides logical characterizations of various forms of entanglement. The logic has been used to specify and verify the correctness of various protocols in quantum computation.[50][51]

Q language

Q Language is the second implemented imperative quantum programming language.[52] Q Language was implemented as an extension of C++ programming language. It provides classes for basic quantum operations like QHadamard, QFourier, QNot, and QSwap, which are derived from the base class Qop. New operators can be defined using C++ class mechanism.

Quantum memory is represented by class Qreg.

```
Qreg x1; // 1-qubit quantum register with initial value 0
Qreg x2(2,0); // 2-qubit quantum register with initial value 0
```

The computation process is executed using a provided simulator. Noisy environments can be simulated using parameters of the simulator.

Q#

A language developed by Microsoft to be used with the Quantum Development Kit.[53]

QCL

Quantum Computation Language (QCL) is one of the first implemented quantum programming languages.[54] The most important feature of QCL is the support for user-defined operators and functions. Its syntax resembles the syntax of the C programming language and its classical data types are similar to primitive data types in C. One can combine classical code and quantum code in the same program.

qGCL

Quantum Guarded Command Language (qGCL) was defined by P. Zuliani in his PhD thesis. It is based on Guarded Command Language created by Edsger Dijkstra.

It can be described as a language of quantum programs specification.

QMASM

Quantum Macro Assembler (QMASM) is a low-level language specific to quantum annealers such as the D-Wave.[55]

Qmod

Quantum Modeling (Qmod) language is a high-level language that abstracts away the gate-level qubit operation, providing a functional approach to the implementation of quantum algorithms on quantum registers. The language is part of the Classiq (https://classiq.io) platform and can be used directly with its native syntax, through a Python SDK, or with a visual editor, all methods can take advantage of the larger library of algorithms and the efficient circuit optimization.

Q|SI>

Q|SI> is a platform embedded in .Net language supporting quantum programming in a quantum extension of while-language.[47][56] This platform includes a compiler of the quantum while-language[57] and a chain of tools for the simulation of quantum computation, optimisation of quantum circuits, termination analysis of quantum programs,[58] and verification of quantum programs.[59][60]

Quantum pseudocode

Quantum pseudocode proposed by E. Knill is the first formalized language for description of quantum algorithms. It was introduced and, moreover, was tightly connected with a model of quantum machine called Quantum Random Access Machine (QRAM).

Scaffold

Scaffold is C-like language, that compiles to QASM and OpenQASM. It is built on top of the LLVM Compiler Infrastructure to perform optimizations on Scaffold code before generating a specified instruction set.[61][62]

Silq

Silq is a high-level programming language for quantum computing with a strong static type system, developed at ETH Zürich.[63][64]

Functional languages

Efforts are underway to develop functional programming languages for quantum computing. Functional programming languages are well-suited for reasoning about programs. Examples include Selinger's QPL,[65] and the Haskell-like language QML by Altenkirch and Grattage.[66][67] Higher-order quantum programming languages, based on lambda calculus, have been proposed by van Tonder,[68] Selinger and Valiron[69] and by Arrighi and Dowek.[70]

LIQUi|>

LIQUi|> (pronounced *liquid*) is a quantum simulation extension on the F# programming language.[71] It is currently being developed by the Quantum Architectures and Computation Group (QuArC)[72] part of the StationQ efforts at Microsoft Research. LIQUi|> seeks to allow theorists to experiment with quantum algorithm design before physical quantum computers are available for use.[73]

It includes a programming language, optimization and scheduling algorithms, and quantum simulators. LIQUi|> can be used to translate a quantum algorithm written in the form of a high-level program into the low-level machine instructions for a quantum device.[74]

QFC and QPL

QFC and QPL are two closely related quantum programming languages defined by Peter Selinger. They differ only in their syntax: QFC uses a flow chart syntax, whereas QPL uses a textual syntax. These languages have classical control flow but can operate on quantum or classical data. Selinger gives a denotational semantics for these languages in a category of superoperators.

QML

QML is a Haskell-like quantum programming language by Altenkirch and Grattage.[75][66] Unlike Selinger's QPL, this language takes duplication, rather than discarding, of quantum information as a primitive operation. Duplication in this context is understood to be the operation that maps $|\phi\rangle$ to $|\phi\rangle \otimes |\phi\rangle$, and is not to be confused with the impossible operation of cloning; the authors claim it is akin to how sharing is modeled in classical languages. QML also introduces both classical and quantum control operators, whereas most other languages rely on classical control.

An operational semantics for QML is given in terms of quantum circuits, while a denotational semantics is presented in terms of superoperators, and these are shown to agree. Both the operational and denotational semantics have been implemented (classically) in Haskell.[76]

Quantum lambda calculi

Quantum lambda calculi are extensions of the classical lambda calculus introduced by Alonzo Church and Stephen Cole Kleene in the 1930s. The purpose of quantum lambda calculi is to extend quantum programming languages with a theory of higher-order functions.

The first attempt to define a quantum lambda calculus was made by Philip Maymin in 1996.[77] His lambda-q calculus is powerful enough to express any quantum computation. However, this language can efficiently solve NP-complete problems, and therefore appears to be strictly stronger than the standard

quantum computational models (such as the quantum Turing machine or the quantum circuit model). Therefore, Maymin's lambda-q calculus is probably not implementable on a physical device .

In 2003, André van Tonder defined an extension of the lambda calculus suitable for proving correctness of quantum programs. He also provided an implementation in the Scheme programming language.[78]

In 2004, Selinger and Valiron defined a strongly typed lambda calculus for quantum computation with a type system based on linear logic.[79]

Quipper

Quipper was published in 2013.[80][81] It is implemented as an embedded language, using Haskell as the host language.[82] For this reason, quantum programs written in Quipper are written in Haskell using provided libraries. For example, the following code implements preparation of a superposition

```
import Quipper

spos :: Bool -> Circ Qubit
spos b = do q <- qinit b
            r <- hadamard q
            return r
```

References

1. Jarosław Adam Miszczak (2012). *High-level Structures in Quantum Computing*. Morgan & Claypool Publishers. ISBN 9781608458516.
2. "Comprehensive list of quantum open-source projects" (https://github.com/qosf/awesome-quantum-software). *Github*. Retrieved January 27, 2022.
3. "Blackbird Quantum Assembly Language — Blackbird 0.2.0 documentation" (https://quantum-blackbird.readthedocs.io/en/latest/). *quantum-blackbird.readthedocs.io*. Retrieved June 24, 2019.
4. Weedbrook, Christian; Amy, Matthew; Bergholm, Ville; Quesada, Nicolás; Izaac, Josh; Killoran, Nathan (March 11, 2019). "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum*. **3**: 129. arXiv:1804.03159 (https://arxiv.org/abs/1804.03159). Bibcode:2019Quant...3..129K (https://ui.adsabs.harvard.edu/abs/2019Quant...3..129K). doi:10.22331/q-2019-03-11-129 (https://doi.org/10.22331%2Fq-2019-03-11-129). S2CID 54763305 (https://api.semanticscholar.org/CorpusID:54763305).
5. Bertels, K.; Almudever, C. G.; Hogaboam, J. W.; Ashraf, I.; Guerreschi, G. G.; Khammassi, N. (May 24, 2018). "cQASM v1.0: Towards a Common Quantum Assembly Language". arXiv:1805.09607v1 (https://arxiv.org/abs/1805.09607v1) [quant-ph (https://arxiv.org/archive/quant-ph)].
6. *qiskit-openqasm: OpenQASM specification* (https://github.com/IBM/qiskit-openqasm), International Business Machines, July 4, 2017, retrieved July 6, 2017
7. Smith, Robert S.; Curtis, Michael J.; Zeng, William J. (2016). "A Practical Quantum Instruction Set Architecture". arXiv:1608.03355 (https://arxiv.org/abs/1608.03355) [quant-ph (https://arxiv.org/archive/quant-ph)].

8. McClean, Jarrod R.; Romero, Jonathan; Babbush, Ryan; Aspuru-Guzik, Alán (February 4, 2016). "The theory of variational hybrid quantum-classical algorithms". *New Journal of Physics*. **18** (2): 023023. arXiv:1509.04279 (https://arxiv.org/abs/1509.04279). Bibcode:2016NJPh...18b3023M (https://ui.adsabs.harvard.edu/abs/2016NJPh...18b3023M). doi:10.1088/1367-2630/18/2/023023 (https://doi.org/10.1088%2F1367-2630%2F18%2F2%2F023023). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 92988541 (https://api.semanticscholar.org/CorpusID:92988541).
9. Rubin, Nicholas C.; Curtis, Michael J.; Zeng, William J. (2016). "A Hybrid Classical/Quantum Approach for Large-Scale Studies of Quantum Systems with Density Matrix Embedding Theory". arXiv:1610.06910 (https://arxiv.org/abs/1610.06910) [quant-ph (https://arxiv.org/archive/quant-ph)].
10. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
11. Häner, Thomas; Steiger, Damian S.; Svore, Krysta; Troyer, Matthias (2018). "A software methodology for compiling quantum programs". *Quantum Science and Technology*. **3** (2): 020501. arXiv:1604.01401 (https://arxiv.org/abs/1604.01401). Bibcode:2018QS&T....3b0501H (https://ui.adsabs.harvard.edu/abs/2018QS&T....3b0501H). doi:10.1088/2058-9565/aaa5cc (https://doi.org/10.1088%2F2058-9565%2Faaa5cc). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 1922315 (https://api.semanticscholar.org/CorpusID:1922315).
12. "PASQAL" (https://pasqal.io/). *PASQAL*.
13. "Home" (https://www.aqt.eu/). *AQT | ALPINE QUANTUM TECHNOLOGIES*.
14. "Welcome to the Documentation for Grove! — Grove 1.7.0 documentation" (https://grove-docs.readthedocs.io/en/latest/). *grove-docs.readthedocs.io*.
15. "MindSpore Quantum Documentation" (https://www.mindspore.cn/mindquantum/docs/en/master/index.html). *www.mindspore.cn/mindquantum*.
16. Xu, Xusheng; et al. (2024). "MindSpore Quantum: A User-Friendly, High-Performance, and AI-Compatible Quantum Computing Framework". arXiv:2406.17248 (https://arxiv.org/abs/2406.17248) [quant-ph (https://arxiv.org/archive/quant-ph)].
17. "mindquantum" (https://github.com/mindspore-ai/mindquantum). *github.com*.
18. "PennyLane Documentation — PennyLane 0.14.1 documentation" (https://pennylane.readthedocs.io/en/stable/). *pennylane.readthedocs.io*. Retrieved March 26, 2021.
19. "AWS joins PennyLane, an open-source framework that melds machine learning with quantum computing" (https://siliconangle.com/2021/02/17/aws-throws-weight-behind-pennylane-open-source-framework-melds-machine-learning-quantum-computing/). *SiliconANGLE*. February 17, 2021. Retrieved March 26, 2021.
20. "SD Times Open-Source Project of the Week: PennyLane" (https://sdtimes.com/open-source/sd-times-open-source-project-of-the-week-pennylane/). *SD Times*. February 26, 2021. Retrieved March 26, 2021.
21. Salamone, Salvatore (December 13, 2020). "Real-time Analytics News Roundup for Week Ending December 12" (https://www.rtinsights.com/real-time-analytics-news-roundup-for-week-ending-december-12/). *RTInsights*. Retrieved March 26, 2021.
22. "Accelerating Quantum Computing" (https://www.quantinuum.com/). *www.quantinuum.com*.
23. "Plugins and ecosystem — PennyLane" (https://pennylane.ai/plugins.html). *pennylane.ai*. Retrieved March 26, 2021.
24. "La puissance d'un ordinateur quantique testée en ligne (The power of a quantum computer tested online)" (https://www.lemonde.fr/sciences/article/2022/11/22/la-puissance-d-un-ordinateur-quantique-testee-en-ligne_6151063_1650684.html). *Le Monde.fr*. Le Monde. November 22, 2022.

25. Heurtel, Nicolas; Fyrillas, Andreas; de Gliniasty, Grégoire; Le Bihan, Raphaël; Malherbe, Sébastien; Pailhas, Marceau; Bertasi, Eric; Bourdoncle, Boris; Emeriau, Pierre-Emmanuel; Mezher, Rawad; Music, Luka; Belabas, Nadia; Valiron, Benoît; Senellart, Pascale; Mansfield, Shane; Senellart, Jean (February 21, 2023). "Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing" (https://quantum-journal.org/papers/q-2023-02-21-931/). *Quantum*. **7**: 931. arXiv:2204.00602 (https://arxiv.org/abs/2204.00602). Bibcode:2023Quant...7..931H (https://ui.adsabs.harvard.edu/abs/2023Quant...7..931H). doi:10.22331/q-2023-02-21-931 (https://doi.org/10.22331%2Fq-2023-02-21-931). S2CID 247922568 (https://api.semanticscholar.org/CorpusID:247922568).
26. "Home" (https://projectq.ch/).
27. Efthymiou, Stavros; Ramos-Calderer, Sergi; Bravo-Prieto, Carlos; Pérez-Salinas, Adrián; García-Martín, Diego; Garcia-Saez, Artur; Latorre, José Ignacio; Carrazza, Stefano (January 1, 2022). "Qibo: a framework for quantum simulation with hardware acceleration" (https://iopscience.iop.org/article/10.1088/2058-9565/ac39f5). *Quantum Science and Technology*. **7** (1): 015018. arXiv:2009.01845 (https://arxiv.org/abs/2009.01845). Bibcode:2022QS&T....7a5018E (https://ui.adsabs.harvard.edu/abs/2022QS&T....7a5018E). doi:10.1088/2058-9565/ac39f5 (https://doi.org/10.1088%2F2058-9565%2Fac39f5). hdl:2434/887963 (https://hdl.handle.net/2434%2F887963). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 221507478 (https://api.semanticscholar.org/CorpusID:221507478).
28. Efthymiou, Stavros; Lazzarin, Marco; Pasquale, Andrea; Carrazza, Stefano (September 22, 2022). "Quantum simulation with just-in-time compilation" (https://quantum-journal.org/papers/q-2022-09-22-814/). *Quantum*. **6**: 814. arXiv:2203.08826 (https://arxiv.org/abs/2203.08826). Bibcode:2022Quant...6..814E (https://ui.adsabs.harvard.edu/abs/2022Quant...6..814E). doi:10.22331/q-2022-09-22-814 (https://doi.org/10.22331%2Fq-2022-09-22-814). S2CID 247518955 (https://api.semanticscholar.org/CorpusID:247518955).
29. "Qibolab" (https://github.com/qiboteam/qibolab). November 2, 2022 – via GitHub.
30. "Qibocal" (https://github.com/qiboteam/qibocal). November 1, 2022 – via GitHub.
31. "qiskit.org" (https://qiskit.org/). *qiskit.org*.
32. "Qiskit Overview" (https://qiskit.org/overview/). Retrieved February 10, 2021.
33. McKay, David C.; Alexander, Thomas; Bello, Luciano; Biercuk, Michael J.; Bishop, Lev; Chen, Jiayin; Chow, Jerry M.; Córcoles, Antonio D.; Egger, Daniel; Filipp, Stefan; Gomez, Juan; Hush, Michael; Javadi-Abhari, Ali; Moreda, Diego; Nation, Paul; Paulovicks, Brent; Winston, Erick; Wood, Christopher J.; Wootton, James; Gambetta, Jay M. (2018). "Qiskit Backend Specifications for OpenQASM and OpenPulse Experiments". arXiv:1809.03452 (https://arxiv.org/abs/1809.03452) [quant-ph (https://arxiv.org/archive/quant-ph)].
34. "Qrisp official website" (https://www.qrisp.eu/).
35. "Eclipse Foundation (website)" (https://www.eclipse.org/org/foundation/).
36. "Fraunhofer FOKUS (website)" (https://www.fokus.fraunhofer.de/).
37. "Azure Quantum documentation, QDK & Q# API reference - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/). *learn.microsoft.com*.
38. "What is Azure Quantum? - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum). *learn.microsoft.com*. January 11, 2023.
39. "Strawberry Fields — Strawberry Fields 0.8.0 documentation" (https://strawberryfields.readthedocs.io/en/latest/). *strawberryfields.readthedocs.io*. Retrieved September 25, 2018.
40. Killoran, Nathan; Izaac, Josh; Quesada, Nicolás; Bergholm, Ville; Amy, Matthew; Weedbrook, Christian (2019). "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum*. **3**: 129. arXiv:1804.03159 (https://arxiv.org/abs/1804.03159). Bibcode:2019Quant...3..129K (https://ui.adsabs.harvard.edu/abs/2019Quant...3..129K). doi:10.22331/q-2019-03-11-129 (https://doi.org/10.22331%2Fq-2019-03-11-129). S2CID 54763305 (https://api.semanticscholar.org/CorpusID:54763305).

41. Weedbrook, Christian; Pirandola, Stefano; García-Patrón, Raúl; Cerf, Nicolas J.; Ralph, Timothy C.; Shapiro, Jeffrey H.; Lloyd, Seth (May 1, 2012). "Gaussian quantum information". *Reviews of Modern Physics*. **84** (2): 621–669. arXiv:1110.3234 (https://arxiv.org/abs/1110.3234). Bibcode:2012RvMP...84..621W (https://ui.adsabs.harvard.edu/abs/2012RvMP...84..621W). doi:10.1103/RevModPhys.84.621 (https://doi.org/10.1103%2FRevModPhys.84.621). S2CID 119250535 (https://api.semanticscholar.org/CorpusID:119250535).
42. "Hardware — Strawberry Fields" (https://strawberryfields.ai/photonics/hardware/index.html). *strawberryfields.ai*. Retrieved March 26, 2021.
43. "In the Race to Hundreds of Qubits, Photons May Have "Quantum Advantage" " (https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon). *IEEE Spectrum: Technology, Engineering, and Science News*. March 5, 2021. Retrieved March 26, 2021.
44. "pytket" (https://github.com/CQCL/pytket). *GitHub*. January 22, 2022.
45. Bernhard Omer. "The QCL Programming Language" (http://tph.tuwien.ac.at/~oemer/qcl.html).
46. Hynek Mlnařík. "LanQ – a quantum imperative programming language" (http://lanq.sourceforge.net/).
47. Liu, Shusen; Zhou, li; Guan, Ji; He, Yang; Duan, Runyao; Ying, Mingsheng (May 9, 2017). "Q|SI>: A Quantum Programming Language". *Scientia Sinica Informationis*. **47** (10): 1300. arXiv:1710.09500 (https://arxiv.org/abs/1710.09500). doi:10.1360/N112017-00095 (https://doi.org/10.1360%2FN112017-00095). S2CID 9163705 (https://api.semanticscholar.org/CorpusID:9163705).
48. Da Rosa, Evandro Chagas Ribeiro; De Santiago, Rafael (January 31, 2022). "Ket Quantum Programming" (https://dl.acm.org/doi/10.1145/3474224). *ACM Journal on Emerging Technologies in Computing Systems*. **18** (1): 1–25. doi:10.1145/3474224 (https://doi.org/10.1145%2F3474224). ISSN 1550-4832 (https://search.worldcat.org/issn/1550-4832).
49. "Ket Quantum Programming" (https://quantumket.org). *quantumket.org*. Retrieved May 18, 2023.
50. A. Baltag and S. Smets, "LQP: The Dynamic Logic of Quantum Information" (https://arxiv.org/abs/2110.01361), Mathematical Structures in Computer Science 16(3):491-525, 2006.
51. Baltag, Alexandru; Bergfeld, Jort; Kishida, Kohei; Sack, Joshua; Smets, Sonja; Zhong, Shengyang (2014). "PLQP & Company: Decidable Logics for Quantum Algorithms" (https://link.springer.com/article/10.1007/s10773-013-1987-3). *International Journal of Theoretical Physics*. **53** (10): 3628–3647. Bibcode:2014IJTP...53.3628B (https://ui.adsabs.harvard.edu/abs/2014IJTP...53.3628B). doi:10.1007/s10773-013-1987-3 (https://doi.org/10.1007%2Fs10773-013-1987-3). S2CID 254573992 (https://api.semanticscholar.org/CorpusID:254573992).
52. "Software for the Q language" (https://web.archive.org/web/20090620011647/http://sra.itc.it/people/serafini/qlang/). November 23, 2001. Archived from the original (http://sra.itc.it/people/serafini/qlang/) on June 20, 2009. Retrieved July 20, 2017.
53. "Introduction to Q# & Quantum Development Kit - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk). *learn.microsoft.com*. March 30, 2023.
54. "QCL - A Programming Language for Quantum Computers" (http://tph.tuwien.ac.at/~oemer/qcl.html). *tuwien.ac.at*. Retrieved July 20, 2017.
55. Scott Pakin, "A Quantum Macro Assembler" (https://ieeexplore.ieee.org/document/7761637/), Proceedings of the 20th Annual IEEE High Performance Extreme Computing Conference 2016
56. Ying, Mingsheng (January 2012). "Floyd–hoare Logic for Quantum Programs" (https://doi.org/10.1145%2F2049706.2049708). *ACM Trans. Program. Lang. Syst*. **33** (6): 19:1–19:49. doi:10.1145/2049706.2049708 (https://doi.org/10.1145%2F2049706.2049708). ISSN 0164-0925 (https://search.worldcat.org/issn/0164-0925). S2CID 416960 (https://api.semanticscholar.org/CorpusID:416960).

57. Ying, Mingsheng; Feng, Yuan (2010). "A Flowchart Language for Quantum Programming" (https://www.computer.org/csdl/trans/ts/2011/04/tts2011040466-abs.html). *IEEE Transactions on Software Engineering*. **37** (4): 466–485. doi:10.1109/TSE.2010.94 (https://doi.org/10.1109%2FTSE.2010.94). ISSN 0098-5589 (https://search.worldcat.org/issn/0098-5589). S2CID 5879273 (https://api.semanticscholar.org/CorpusID:5879273).
58. Ying, Mingsheng; Yu, Nengkun; Feng, Yuan; Duan, Runyao (2013). "Verification of quantum programs". *Science of Computer Programming*. **78** (9): 1679–1700. arXiv:1106.4063 (https://arxiv.org/abs/1106.4063). doi:10.1016/j.scico.2013.03.016 (https://doi.org/10.1016%2Fj.scico.2013.03.016). S2CID 18913620 (https://api.semanticscholar.org/CorpusID:18913620).
59. Ying, Mingsheng; Ying, Shenggang; Wu, Xiaodi (2017), "Invariants of quantum programs: Characterisations and generation", *ACM SIGPLAN Notices*, **52**: 818–832, doi:10.1145/3093333.3009840 (https://doi.org/10.1145%2F3093333.3009840), hdl:10453/127333 (https://hdl.handle.net/10453%2F127333)
60. Liu, Tao; Li, Yangjia; Wang, Shuling; Ying, Mingsheng; Zhan, Naijun (2016). "A Theorem Prover for Quantum Hoare Logic and its Applications". arXiv:1601.03835 (https://arxiv.org/abs/1601.03835) [cs.LO (https://arxiv.org/archive/cs.LO)].
61. Javadi-Abhari, Ali. "Scaffold: Quantum Programming Language" (https://www.cs.princeton.edu/research/techreps/TR-934-12). *Princeton University-Department of Computer Science*. Princeton University. Retrieved September 22, 2020.
62. Litteken, Andrew (May 28, 2020). "An updated LLVM-based quantum research compiler with further OpenQASM support" (https://doi.org/10.1088%2F2058-9565%2Fab8c2c). *Quantum Science and Technology*. **5** (3): 034013. Bibcode:2020QS&T....5c4013L (https://ui.adsabs.harvard.edu/abs/2020QS&T....5c4013L). doi:10.1088/2058-9565/ab8c2c (https://doi.org/10.1088%2F2058-9565%2Fab8c2c). OSTI 1803951 (https://www.osti.gov/biblio/1803951). S2CID 219101628 (https://api.semanticscholar.org/CorpusID:219101628).
63. "What is Silq?" (https://silq.ethz.ch/). *silq.ethz.ch*. Retrieved June 21, 2020.
64. Bichsel, Benjamin; Baader, Maximilian; Gehr, Timon; Vechev, Martin (June 11, 2020). "Silq: A high-level quantum language with safe uncomputation and intuitive semantics". *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*. London UK: ACM. pp. 286–300. doi:10.1145/3385412.3386007 (https://doi.org/10.1145%2F3385412.3386007). ISBN 978-1-4503-7613-6. S2CID 219397029 (https://api.semanticscholar.org/CorpusID:219397029).
65. Peter Selinger, "Towards a quantum programming language" (http://www.mathstat.dal.ca/~selinger/papers.html#qpl), Mathematical Structures in Computer Science 14(4):527-586, 2004.
66. Jonathan Grattage: QML Research (http://www.cs.nott.ac.uk/~jjg/qml.html) (website)
67. T. Altenkirch, V. Belavkin, J. Grattage, A. Green, A. Sabry, J. K. Vizzotto, QML: A Functional Quantum Programming Language (http://sneezy.cs.nott.ac.uk/qml) Archived (https://web.archive.org/web/20060710201728/http://sneezy.cs.nott.ac.uk/QML/) 2006-07-10 at the Wayback Machine (website)
68. Andre van Tonder, "A Lambda Calculus for Quantum Computation" (https://dx.doi.org/10.1137/S0097539703432165), SIAM J. Comput., 33(5), 1109–1135. (27 pages), 2004. Also available from arXiv:quant-ph/0307150 (https://arxiv.org/abs/quant-ph/0307150)
69. Peter Selinger and Benoît Valiron, "A lambda calculus for quantum computation with classical control" (http://www.mathstat.dal.ca/~selinger/papers/#qlambda), Mathematical Structures in Computer Science 16(3):527-552, 2006.
70. Pablo Arrighi, Gilles Dowek, "Linear-algebraic lambda-calculus: higher-order, encodings and confluence" (http://www.arxiv.org/abs/quant-ph/0612199), 2006
71. "The Language Integrated Quantum Operations Simulator" (https://stationq.github.io/Liquid/). *github.io*. Retrieved July 20, 2017.
72. Quantum Architectures and Computation Group (QuArC), https://www.microsoft.com/en-us/research/group/quantum-architectures-and-computation-group-quarc/, 2011

73. "StationQ" (https://stationq.microsoft.com/). *microsoft.com*. Retrieved July 20, 2017.
74. "Language-Integrated Quantum Operations: LIQUi|>" (https://www.microsoft.com/en-us/research/project/language-integrated-quantum-operations-liqui/). *Microsoft*. 2016.
75. "QML: A Functional Quantum Programming Language" (https://web.archive.org/web/20070926230222/http://sneezy.cs.nott.ac.uk/QML/). September 26, 2007. Archived from the original (http://sneezy.cs.nott.ac.uk/QML/) on September 26, 2007.
76. Jonathan Grattage, QML: A Functional Quantum Programming Language (compiler) (http://sneezy.cs.nott.ac.uk/qml/compiler) Archived (https://web.archive.org/web/20160305052237/http://sneezy.cs.nott.ac.uk/qml/compiler/) 2016-03-05 at the Wayback Machine, 2005–2008
77. Philip Maymin, "Extending the Lambda Calculus to Express Randomized and Quantumized Algorithms" (https://arxiv.org/abs/quant-ph/9612052), 1996
78. André van Tonder. "A lambda calculus for quantum computation (website)" (https://web.archive.org/web/20160305100936/http://www.het.brown.edu/people/andre/qlambda/). Archived from the original (http://www.het.brown.edu/people/andre/qlambda) on March 5, 2016. Retrieved October 2, 2007.
79. Peter Selinger, Benoˆıt Valiron, "Quantum Lambda Calculus" (https://www.mscs.dal.ca/~selinger/papers/qlambdabook.pdf)
80. "The Quipper Language" (http://www.mathstat.dal.ca/~selinger/quipper/).
81. Alexander S. Green; Peter LeFanu Lumsdaine; Neil J. Ross; Peter Selinger; Benoît Valiron. "The Quipper Language (website)" (http://www.mathstat.dal.ca/~selinger/quipper/).
82. Alexander S. Green; Peter LeFanu Lumsdaine; Neil J. Ross; Peter Selinger; Benoît Valiron (2013). "An Introduction to Quantum Programming in Quipper". *Reversible Computation*. Lecture Notes in Computer Science. Vol. 7948. pp. 110–124. arXiv:1304.5485 (https://arxiv.org/abs/1304.5485). doi:10.1007/978-3-642-38986-3_10 (https://doi.org/10.1007%2F978-3-642-38986-3_10). ISBN 978-3-642-38985-6. S2CID 9135905 (https://api.semanticscholar.org/CorpusID:9135905).

Further reading

- Mingsheng, Ying (2024). *Foundations of quantum programming* (2nd ed.). Cambridge, Massachusetts: Morgan Kaufmann. ISBN 978-0-4431-5942-8. OCLC 1406095194 (https://search.worldcat.org/oclc/1406095194). 978-0-4431-5943-5 (eBook).
- Serrano, Manuel A.; Pérez-Castillo, Ricardo; Piattini, Mario, eds. (2022). *Quantum Software Engineering* (1st ed.). Cham, Switzerland: Springer. doi:10.1007/978-3-031-05324-5 (https://doi.org/10.1007%2F978-3-031-05324-5). ISBN 978-3-031-05323-8. OCLC 1347696597 (https://search.worldcat.org/oclc/1347696597). 978-3-031-05326-9 (softcover) & 978-3-031-05324-5 (eBook).

External links

- Curated list (https://github.com/qosf/awesome-quantum-software) of all quantum open-source software projects
- Bibliography on Quantum Programming Languages (http://www.dcs.gla.ac.uk/~simon/quantum/) (updated in May 2007)
- Quantum Physics and Logic (QPL) Conference Series (https://www.mathstat.dal.ca/~selinger/qpl/) (L stood for 'Languages' until 2006)
- Quantum programming language (https://quantiki.org/wiki/quantum-programming-language) in Quantiki (http://www.quantiki.org/)
- QMASM documentation (https://github.com/lanl/qmasm/wiki)

- pyQuil documentation (https://pyquil.readthedocs.io/en/stable/index.html) including Introduction to Quantum Computing (https://pyquil.readthedocs.io/en/stable/intro.html) Archived (https://web.archive.org/web/20180718165337/https://pyquil.readthedocs.io/en/stable/intro.html) July 18, 2018, at the Wayback Machine
- Scaffold Source (https://github.com/epiqc/ScaffCC)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_programming&oldid=1241083092"

WIKIPEDIA
The Free Encyclopedia

Quantum simulator

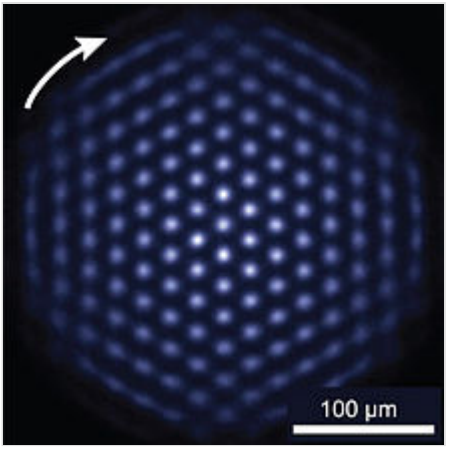
Quantum simulators permit the study of a quantum system in a programmable fashion. In this instance, simulators are special purpose devices designed to provide insight about specific physics problems.[1][2][3] Quantum simulators may be contrasted with generally programmable "digital" quantum computers, which would be capable of solving a wider class of quantum problems.

A **universal quantum simulator** is a quantum computer proposed by Yuri Manin in 1980[4] and Richard Feynman in 1982.[5]

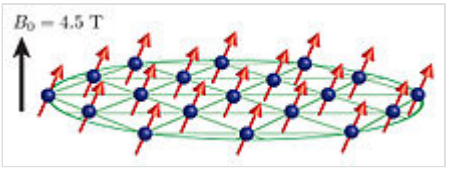
A quantum system may be simulated by either a Turing machine or a quantum Turing machine, as a classical Turing machine is able to simulate a universal quantum computer (and therefore any simpler quantum simulator), meaning they are equivalent from the point of view of computability theory. The simulation of a quantum physics by a classical computer has been shown to be inefficient.[6] In other words, quantum computers provide no additional *power* over classical computers in terms of computability, but it is suspected that they can solve certain problems faster than classical computers, meaning they may be in different complexity classes, which is why quantum Turing machines are useful for simulating quantum systems. This is known as quantum supremacy, the idea that there are problems only quantum Turing machines can solve in any *feasible* amount of time.

A quantum system of many particles could be simulated by a quantum computer using a number of quantum bits similar to the number of particles in the original system.[5] This has been extended to much larger classes of quantum systems.[7][8][9][10]

Quantum simulators have been realized on a number of experimental platforms, including systems of ultracold quantum gases, polar molecules, trapped ions, photonic systems, quantum dots, and superconducting circuits.[11]



In this photograph of a quantum simulator crystal the ions are fluorescing, indicating the qubits are all in the same state (either "1" or "0"). Under the right experimental conditions, the ion crystal spontaneously forms this nearly perfect triangular lattice structure. *Credit: Britton/NIST*



Trapped ion quantum simulator illustration: The heart of the simulator is a two-dimensional crystal of beryllium ions (blue spheres in the graphic); the outermost electron of each ion is a quantum bit (qubit, red arrows). The ions are confined by a large magnetic field in a device called a Penning trap (not shown). Inside the trap the crystal rotates clockwise. *Credit: Britton/NIST*

Solving physics problems

Many important problems in physics, especially low-temperature physics and many-body physics, remain poorly understood because the underlying quantum mechanics is vastly complex. Conventional computers, including supercomputers, are inadequate for simulating quantum systems with as few as 30

particles because the dimension of the Hilbert space grows exponentially with particle number.[12] Better computational tools are needed to understand and rationally design materials whose properties are believed to depend on the collective quantum behavior of hundreds of particles.[2][3] Quantum simulators provide an alternative route to understanding the properties of these systems. These simulators create clean realizations of specific systems of interest, which allows precise realizations of their properties. Precise control over and broad tunability of parameters of the system allows the influence of various parameters to be cleanly disentangled.

Quantum simulators can solve problems which are difficult to simulate on classical computers because they directly exploit quantum properties of real particles. In particular, they exploit a property of quantum mechanics called superposition, wherein a quantum particle is made to be in two distinct states at the same time, for example, aligned and anti-aligned with an external magnetic field. Crucially, simulators also take advantage of a second quantum property called entanglement, allowing the behavior of even physically well separated particles to be correlated.[2][3][13]

Recently quantum simulators have been used to obtain time crystals[14][15] and quantum spin liquids.[16][17]

Trapped-ion simulators

Ion trap based system forms an ideal setting for simulating interactions in quantum spin models.[18] A trapped-ion simulator, built by a team that included the NIST can engineer and control interactions among hundreds of quantum bits (qubits).[19] Previous endeavors were unable to go beyond 30 quantum bits. The capability of this simulator is 10 times more than previous devices. It has passed a series of important benchmarking tests that indicate a capability to solve problems in material science that are impossible to model on conventional computers.

The trapped-ion simulator consists of a tiny, single-plane crystal of hundreds of beryllium ions, less than 1 millimeter in diameter, hovering inside a device called a Penning trap. The outermost electron of each ion acts as a tiny quantum magnet and is used as a qubit, the quantum equivalent of a “1” or a “0” in a conventional computer. In the benchmarking experiment, physicists used laser beams to cool the ions to near absolute zero. Carefully timed microwave and laser pulses then caused the qubits to interact, mimicking the quantum behavior of materials otherwise very difficult to study in the laboratory. Although the two systems may outwardly appear dissimilar, their behavior is engineered to be mathematically identical. In this way, simulators allow researchers to vary parameters that couldn’t be changed in natural solids, such as atomic lattice spacing and geometry.

Friedenauer et al., adiabatically manipulated 2 spins, showing their separation into ferromagnetic and antiferromagnetic states.[20] Kim et al., extended the trapped ion quantum simulator to 3 spins, with global antiferromagnetic Ising interactions featuring frustration and showing the link between frustration and entanglement[21] and Islam et al., used adiabatic quantum simulation to demonstrate the sharpening of a phase transition between paramagnetic and ferromagnetic ordering as the number of spins increased from 2 to 9.[22] Barreiro et al. created a digital quantum simulator of interacting spins with up to 5 trapped ions by coupling to an open reservoir[23] and Lanyon *et al.* demonstrated digital quantum simulation with up to 6 ions.[24] Islam, et al., demonstrated adiabatic quantum simulation of the transverse Ising model with variable (long) range interactions with up to 18 trapped ion spins, showing

control of the level of spin frustration by adjusting the antiferromagnetic interaction range.[25] Britton, et al. from NIST has experimentally benchmarked Ising interactions in a system of hundreds of qubits for studies of quantum magnetism.[19] Pagano, et al., reported a new cryogenic ion trapping system designed for long time storage of large ion chains demonstrating coherent one and two-qubit operations for chains of up to 44 ions.[26] Joshi, et al., probed the quantum dynamics of 51 individually controlled ions, realizing a long-range interacting spin chain.[27]

Ultracold atom simulators

Many ultracold atom experiments are examples of quantum simulators. These include experiments studying bosons or fermions in optical lattices, the unitary Fermi gas, Rydberg atom arrays in optical tweezers. A common thread for these experiments is the capability of realizing generic Hamiltonians, such as the Hubbard or transverse-field Ising Hamiltonian. Major aims of these experiments include identifying low-temperature phases or tracking out-of-equilibrium dynamics for various models, problems which are theoretically and numerically intractable.[28][29] Other experiments have realized condensed matter models in regimes which are difficult or impossible to realize with conventional materials, such as the Haldane model and the Harper-Hofstadter model.[30][31][32][33][34]

Superconducting qubits

Quantum simulators using superconducting qubits fall into two main categories. First, so called quantum annealers determine ground states of certain Hamiltonians after an adiabatic ramp. This approach is sometimes called adiabatic quantum computing. Second, many systems emulate specific Hamiltonians and study their ground state properties, quantum phase transitions, or time dynamics.[35] Several important recent results include the realization of a Mott insulator in a driven-dissipative Bose-Hubbard system and studies of phase transitions in lattices of superconducting resonators coupled to qubits.[36][37]

See also

- Hamiltonian simulation
- Quantum Turing machine
- Quantum computing

References

1. Johnson, Tomi H.; Clark, Stephen R.; Jaksch, Dieter (2014). "What is a quantum simulator?". *EPJ Quantum Technology*. **1** (10). arXiv:1405.2831 (https://arxiv.org/abs/1405.2831). doi:10.1140/epjqt10 (https://doi.org/10.1140%2Fepjqt10). S2CID 120250321 (https://api.semanticscholar.org/CorpusID:120250321).
2. This article incorporates public domain material from Michael E. Newman. *NIST Physicists Benchmark Quantum Simulator with Hundreds of Qubits* (https://www.nist.gov/public_affairs/tech-beat/tb20120502.cfm/). National Institute of Standards and Technology. Retrieved 2013-02-22.

3. Britton, Joseph W.; Sawyer, Brian C.; Keith, Adam C.; Wang, C.-C. Joseph; Freericks, James K.; Uys, Hermann; Biercuk, Michael J.; Bollinger, John J. (2012). "Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins" (http://tf.boulder.nist.gov/general/pdf/2614.pdf) (PDF). *Nature*. **484** (7395): 489–92. arXiv:1204.5789 (https://arxiv.org/abs/1204.5789). Bibcode:2012Natur.484..489B (https://ui.adsabs.harvard.edu/abs/2012Natur.484..489B). doi:10.1038/nature10981 (https://doi.org/10.1038%2Fnature10981). PMID 22538611 (https://pubmed.ncbi.nlm.nih.gov/22538611). S2CID 4370334 (https://api.semanticscholar.org/CorpusID:4370334). Note: This manuscript is a contribution of the US National Institute of Standards and Technology and is not subject to US copyright.
4. Manin, Yu. I. (1980). *Vychislimoe i nevychislimoe* (https://web.archive.org/web/20130510173823/http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) [*Computable and Noncomputable*] (in Russian). Sov.Radio. pp. 13–15. Archived from the original (http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) on 2013-05-10. Retrieved 2013-03-04.
5. Feynman, Richard (1982). "Simulating Physics with Computers". *International Journal of Theoretical Physics*. **21** (6–7): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). CiteSeerX 10.1.1.45.9310 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9310). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445).
6. Feynman, Richard P. (1982-06-01). "Simulating physics with computers" (https://doi.org/10.1007/BF02650179). *International Journal of Theoretical Physics*. **21** (6): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). ISSN 1572-9575 (https://search.worldcat.org/issn/1572-9575). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445).
7. Dorit Aharonov; Amnon Ta-Shma (2003). "Adiabatic Quantum State Generation and Statistical Zero Knowledge". arXiv:quant-ph/0301023 (https://arxiv.org/abs/quant-ph/0301023).
8. Berry, Dominic W.; Graeme Ahokas; Richard Cleve; Sanders, Barry C. (2007). "Efficient quantum algorithms for simulating sparse Hamiltonians". *Communications in Mathematical Physics*. **270** (2): 359–371. arXiv:quant-ph/0508139 (https://arxiv.org/abs/quant-ph/0508139). Bibcode:2007CMaPh.270..359B (https://ui.adsabs.harvard.edu/abs/2007CMaPh.270..359B). doi:10.1007/s00220-006-0150-x (https://doi.org/10.1007%2Fs00220-006-0150-x). S2CID 37923044 (https://api.semanticscholar.org/CorpusID:37923044).
9. Childs, Andrew M. (2010). "On the relationship between continuous- and discrete-time quantum walk". *Communications in Mathematical Physics*. **294** (2): 581–603. arXiv:0810.0312 (https://arxiv.org/abs/0810.0312). Bibcode:2010CMaPh.294..581C (https://ui.adsabs.harvard.edu/abs/2010CMaPh.294..581C). doi:10.1007/s00220-009-0930-1 (https://doi.org/10.1007%2Fs00220-009-0930-1). S2CID 14801066 (https://api.semanticscholar.org/CorpusID:14801066).
10. Kliesch, M.; Barthel, T.; Gogolin, C.; Kastoryano, M.; Eisert, J. (12 September 2011). "Dissipative Quantum Church-Turing Theorem". *Physical Review Letters*. **107** (12): 120501. arXiv:1105.3986 (https://arxiv.org/abs/1105.3986). Bibcode:2011PhRvL.107l0501K (https://ui.adsabs.harvard.edu/abs/2011PhRvL.107l0501K). doi:10.1103/PhysRevLett.107.120501 (https://doi.org/10.1103%2FPhysRevLett.107.120501). PMID 22026760 (https://pubmed.ncbi.nlm.nih.gov/22026760). S2CID 11322270 (https://api.semanticscholar.org/CorpusID:11322270).
11. Nature Physics Insight – Quantum Simulation (http://www.nature.com/nphys/insight/quantum-simulation/index.html#editorial). Nature.com. April 2012.

12. Lloyd, S. (1996). "Universal quantum simulators". *Science*. **273** (5278): 1073–8. Bibcode:1996Sci...273.1073L (https://ui.adsabs.harvard.edu/abs/1996Sci...273.1073L). doi:10.1126/science.273.5278.1073 (https://doi.org/10.1126%2Fscience.273.5278.1073). PMID 8688088 (https://pubmed.ncbi.nlm.nih.gov/8688088). S2CID 43496899 (https://api.semanticscholar.org/CorpusID:43496899).
13. Cirac, J. Ignacio; Zoller, Peter (2012). "Goals and opportunities in quantum simulation" (http://211.144.68.84:9998/91keshi/Public/File/34/8-4/pdf/nphys2275.pdf) (PDF). *Nature Physics*. **8** (4): 264–266. Bibcode:2012NatPh...8..264C (https://ui.adsabs.harvard.edu/abs/2012NatPh...8..264C). doi:10.1038/nphys2275 (https://doi.org/10.1038%2Fnphys2275). S2CID 109930964 (https://api.semanticscholar.org/CorpusID:109930964).
14. Kyprianidis, A.; Machado, F.; Morong, W.; Becker, P.; Collins, K. S.; Else, D. V.; Feng, L.; Hess, P. W.; Nayak, C.; Pagano, G.; Yao, N. Y. (2021-06-11). "Observation of a prethermal discrete time crystal" (https://www.science.org/doi/10.1126/science.abg8102). *Science*. **372** (6547): 1192–1196. arXiv:2102.01695 (https://arxiv.org/abs/2102.01695). Bibcode:2021Sci...372.1192K (https://ui.adsabs.harvard.edu/abs/2021Sci...372.1192K). doi:10.1126/science.abg8102 (https://doi.org/10.1126%2Fscience.abg8102). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 34112691 (https://pubmed.ncbi.nlm.nih.gov/34112691). S2CID 231786633 (https://api.semanticscholar.org/CorpusID:231786633).
15. S, Robert; ers; Berkeley, U. C. (2021-11-10). "Creating Time Crystals Using New Quantum Computing Architectures" (https://scitechdaily.com/creating-time-crystals-using-new-quantum-computing-architectures/). *SciTechDaily*. Retrieved 2021-12-27.
16. Semeghini, G.; Levine, H.; Keesling, A.; Ebadi, S.; Wang, T. T.; Bluvstein, D.; Verresen, R.; Pichler, H.; Kalinowski, M.; Samajdar, R.; Omran, A. (2021-12-03). "Probing topological spin liquids on a programmable quantum simulator" (https://www.science.org/doi/10.1126/science.abi8794). *Science*. **374** (6572): 1242–1247. arXiv:2104.04119 (https://arxiv.org/abs/2104.04119). Bibcode:2021Sci...374.1242S (https://ui.adsabs.harvard.edu/abs/2021Sci...374.1242S). doi:10.1126/science.abi8794 (https://doi.org/10.1126%2Fscience.abi8794). PMID 34855494 (https://pubmed.ncbi.nlm.nih.gov/34855494). S2CID 233204440 (https://api.semanticscholar.org/CorpusID:233204440).
17. Wood, Charlie (2021-12-02). "Quantum Simulators Create a Totally New Phase of Matter" (https://www.quantamagazine.org/quantum-simulators-create-a-totally-new-phase-of-matter-20211202/). *Quanta Magazine*. Retrieved 2022-03-11.
18. Monroe, C; et, al (2021). "Programmable quantum simulations of spin systems with trapped ions". *Rev. Mod. Phys*. **93** (4): 025001. arXiv:1912.07845 (https://arxiv.org/abs/1912.07845). Bibcode:2021RvMP...93b5001M (https://ui.adsabs.harvard.edu/abs/2021RvMP...93b5001M). doi:10.1103/RevModPhys.93.025001 (https://doi.org/10.1103%2FRevModPhys.93.025001). ISSN 0034-6861 (https://search.worldcat.org/issn/0034-6861). S2CID 209386771 (https://api.semanticscholar.org/CorpusID:209386771).
19. Britton, Joseph W.; Sawyer, Brian C.; Keith, Adam C.; Wang, C.-C. Joseph; Freericks, James K.; Uys, Hermann; Biercuk, Michael J.; Bollinger, John J. (25 April 2012). "Engineered two-dimensional Ising interactions in a trapped-ion quantum simulator with hundreds of spins". *Nature*. **484** (7395): 489–492. arXiv:1204.5789 (https://arxiv.org/abs/1204.5789). Bibcode:2012Natur.484..489B (https://ui.adsabs.harvard.edu/abs/2012Natur.484..489B). doi:10.1038/nature10981 (https://doi.org/10.1038%2Fnature10981). PMID 22538611 (https://pubmed.ncbi.nlm.nih.gov/22538611). S2CID 4370334 (https://api.semanticscholar.org/CorpusID:4370334).
20. Friedenauer, A.; Schmitz, H.; Glueckert, J. T.; Porras, D.; Schaetz, T. (27 July 2008). "Simulating a quantum magnet with trapped ions" (https://doi.org/10.1038%2Fnphys1032). *Nature Physics*. **4** (10): 757–761. Bibcode:2008NatPh...4..757F (https://ui.adsabs.harvard.edu/abs/2008NatPh...4..757F). doi:10.1038/nphys1032 (https://doi.org/10.1038%2Fnphys1032).

21. Kim, K.; Chang, M.-S.; Korenblit, S.; Islam, R.; Edwards, E. E.; Freericks, J. K.; Lin, G.-D.; Duan, L.-M.; Monroe, C. (June 2010). "Quantum simulation of frustrated Ising spins with trapped ions". *Nature*. **465** (7298): 590–593. Bibcode:2010Natur.465..590K (https://ui.adsabs.harvard.edu/abs/2010Natur.465..590K). doi:10.1038/nature09071 (https://doi.org/10.1038%2Fnature09071). PMID 20520708 (https://pubmed.ncbi.nlm.nih.gov/20520708). S2CID 2479652 (https://api.semanticscholar.org/CorpusID:2479652).
22. Islam, R.; Edwards, E.E.; Kim, K.; Korenblit, S.; Noh, C.; Carmichael, H.; Lin, G.-D.; Duan, L.-M.; Joseph Wang, C.-C.; Freericks, J.K.; Monroe, C. (5 July 2011). "Onset of a quantum phase transition with a trapped ion quantum simulator". *Nature Communications*. **2** (1): 377. arXiv:1103.2400 (https://arxiv.org/abs/1103.2400). Bibcode:2011NatCo...2..377I (https://ui.adsabs.harvard.edu/abs/2011NatCo...2..377I). doi:10.1038/ncomms1374 (https://doi.org/10.1038%2Fncomms1374). PMID 21730958 (https://pubmed.ncbi.nlm.nih.gov/21730958). S2CID 33407 (https://api.semanticscholar.org/CorpusID:33407).
23. Barreiro, Julio T.; Müller, Markus; Schindler, Philipp; Nigg, Daniel; Monz, Thomas; Chwalla, Michael; Hennrich, Markus; Roos, Christian F.; Zoller, Peter; Blatt, Rainer (23 February 2011). "An open-system quantum simulator with trapped ions". *Nature*. **470** (7335): 486–491. arXiv:1104.1146 (https://arxiv.org/abs/1104.1146). Bibcode:2011Natur.470..486B (https://ui.adsabs.harvard.edu/abs/2011Natur.470..486B). doi:10.1038/nature09801 (https://doi.org/10.1038%2Fnature09801). PMID 21350481 (https://pubmed.ncbi.nlm.nih.gov/21350481). S2CID 4359894 (https://api.semanticscholar.org/CorpusID:4359894).
24. Lanyon, B. P.; Hempel, C.; Nigg, D.; Muller, M.; Gerritsma, R.; Zahringer, F.; Schindler, P.; Barreiro, J. T.; Rambach, M.; Kirchmair, G.; Hennrich, M.; Zoller, P.; Blatt, R.; Roos, C. F. (1 September 2011). "Universal Digital Quantum Simulation with Trapped Ions". *Science*. **334** (6052): 57–61. arXiv:1109.1512 (https://arxiv.org/abs/1109.1512). Bibcode:2011Sci...334...57L (https://ui.adsabs.harvard.edu/abs/2011Sci...334...57L). doi:10.1126/science.1208001 (https://doi.org/10.1126%2Fscience.1208001). PMID 21885735 (https://pubmed.ncbi.nlm.nih.gov/21885735). S2CID 206535076 (https://api.semanticscholar.org/CorpusID:206535076).
25. Islam, R.; Senko, C.; Campbell, W. C.; Korenblit, S.; Smith, J.; Lee, A.; Edwards, E. E.; Wang, C.- C. J.; Freericks, J. K.; Monroe, C. (2 May 2013). "Emergence and Frustration of Magnetism with Variable-Range Interactions in a Quantum Simulator". *Science*. **340** (6132): 583–587. arXiv:1210.0142 (https://arxiv.org/abs/1210.0142). Bibcode:2013Sci...340..583I (https://ui.adsabs.harvard.edu/abs/2013Sci...340..583I). doi:10.1126/science.1232296 (https://doi.org/10.1126%2Fscience.1232296). PMID 23641112 (https://pubmed.ncbi.nlm.nih.gov/23641112). S2CID 14692151 (https://api.semanticscholar.org/CorpusID:14692151).
26. Pagano, G; Hess, P W; Kaplan, H B; Tan, W L; Richerme, P; Becker, P; Kyprianidis, A; Zhang, J; Birckelbaw, E; Hernandez, M R; Wu, Y; Monroe, C (9 October 2018). "Cryogenic trapped-ion system for large scale quantum simulation". *Quantum Science and Technology*. **4** (1): 014004. arXiv:1802.03118 (https://arxiv.org/abs/1802.03118). doi:10.1088/2058-9565/aae0fe (https://doi.org/10.1088%2F2058-9565%2Faae0fe). S2CID 54518534 (https://api.semanticscholar.org/CorpusID:54518534).
27. Joshi, M.K.; Kranzl, F.; Schuckert, A.; Lovas, I.; Maier, C.; Blatt, R.; Knap, M.; Roos, C.F. (13 May 2022). "Observing emergent hydrodynamics in a long-range quantum magnet" (https://www.science.org/doi/10.1126/science.abk2400). *Science*. **6594** (376): 720–724. arXiv:2107.00033 (https://arxiv.org/abs/2107.00033). Bibcode:2022Sci...376..720J (https://ui.adsabs.harvard.edu/abs/2022Sci...376..720J). doi:10.1126/science.abk2400 (https://doi.org/10.1126%2Fscience.abk2400). PMID 35549407 (https://pubmed.ncbi.nlm.nih.gov/35549407). S2CID 235694285 (https://api.semanticscholar.org/CorpusID:235694285). Retrieved 13 May 2022.
28. Bloch, Immanuel; Dalibard, Jean; Nascimbene, Sylvain (2012). "Quantum simulations with ultracold quantum gases". *Nature Physics*. **8** (4): 267–276. Bibcode:2012NatPh...8..267B (https://ui.adsabs.harvard.edu/abs/2012NatPh...8..267B). doi:10.1038/nphys2259 (https://doi.org/10.1038%2Fnphys2259). S2CID 17023076 (https://api.semanticscholar.org/CorpusID:17023076).

29. Gross, Christian; Bloch, Immanuel (September 8, 2017). "Quantum simulations with ultracold atoms in optical lattices" (https://doi.org/10.1126%2Fscience.aal3837). *Nature*. **357** (6355): 995–1001. Bibcode:2017Sci...357..995G (https://ui.adsabs.harvard.edu/abs/2017Sci...357..995G). doi:10.1126/science.aal3837 (https://doi.org/10.1126%2Fscience.aal3837). PMID 28883070 (https://pubmed.ncbi.nlm.nih.gov/28883070).
30. Jotzu, Gregor; Messer, Michael; Desbuquois, Rémi; Lebrat, Martin; Uehlinger, Thomas; Greif, Daniel; Esslinger, Tilman (13 November 2014). "Experimental realization of the topological Haldane model with ultracold fermions". *Nature*. **515** (7526): 237–240. arXiv:1406.7874 (https://arxiv.org/abs/1406.7874). Bibcode:2014Natur.515..237J (https://ui.adsabs.harvard.edu/abs/2014Natur.515..237J). doi:10.1038/nature13915 (https://doi.org/10.1038%2Fnature13915). PMID 25391960 (https://pubmed.ncbi.nlm.nih.gov/25391960). S2CID 204898338 (https://api.semanticscholar.org/CorpusID:204898338).
31. Simon, Jonathan (13 November 2014). "Magnetic fields without magnetic fields" (https://doi.org/10.1038%2F515202a). *Nature*. **515** (7526): 202–203. doi:10.1038/515202a (https://doi.org/10.1038%2F515202a). PMID 25391956 (https://pubmed.ncbi.nlm.nih.gov/25391956).
32. Zhang, Dan-Wei; Zhu, Yan-Qing; Zhao, Y. X.; Yan, Hui; Zhu, Shi-Liang (29 March 2019). "Topological quantum matter with cold atoms". *Advances in Physics*. **67** (4): 253–402. arXiv:1810.09228 (https://arxiv.org/abs/1810.09228). doi:10.1080/00018732.2019.1594094 (https://doi.org/10.1080%2F00018732.2019.1594094). S2CID 91184189 (https://api.semanticscholar.org/CorpusID:91184189).
33. Alberti, Andrea; Robens, Carsten; Alt, Wolfgang; Brakhane, Stefan; Karski, Michał; Reimann, René; Widera, Artur; Meschede, Dieter (2016-05-06). "Super-resolution microscopy of single atoms in optical lattices" (https://doi.org/10.1088%2F1367-2630%2F18%2F5%2F053010). *New Journal of Physics*. **18** (5): 053010. arXiv:1512.07329 (https://arxiv.org/abs/1512.07329). Bibcode:2016NJPh...18e3010A (https://ui.adsabs.harvard.edu/abs/2016NJPh...18e3010A). doi:10.1088/1367-2630/18/5/053010 (https://doi.org/10.1088%2F1367-2630%2F18%2F5%2F053010). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).
34. Robens, Carsten; Brakhane, Stefan; Meschede, Dieter; Alberti, A. (2016-09-18), "Quantum Walks with Neutral Atoms: Quantum Interference Effects of One and Two Particles" (https://www.worldscientific.com/doi/abs/10.1142/9789813200616_0001), *Laser Spectroscopy*, WORLD SCIENTIFIC, pp. 1–15, arXiv:1511.03569 (https://arxiv.org/abs/1511.03569), doi:10.1142/9789813200616_0001 (https://doi.org/10.1142%2F9789813200616_0001), ISBN 978-981-320-060-9, S2CID 118452312 (https://api.semanticscholar.org/CorpusID:118452312), retrieved 2020-05-25
35. Paraoanu, G. S. (4 April 2014). "Recent Progress in Quantum Simulation Using Superconducting Circuits". *Journal of Low Temperature Physics*. **175** (5–6): 633–654. arXiv:1402.1388 (https://arxiv.org/abs/1402.1388). Bibcode:2014JLTP..175..633P (https://ui.adsabs.harvard.edu/abs/2014JLTP..175..633P). doi:10.1007/s10909-014-1175-8 (https://doi.org/10.1007%2Fs10909-014-1175-8). S2CID 119276238 (https://api.semanticscholar.org/CorpusID:119276238).
36. Ma, Ruichao; Saxberg, Brendan; Owens, Clai; Leung, Nelson; Lu, Yao; Simon, Jonathan; Schuster, David I. (6 February 2019). "A dissipatively stabilized Mott insulator of photons". *Nature*. **566** (7742): 51–57. arXiv:1807.11342 (https://arxiv.org/abs/1807.11342). Bibcode:2019Natur.566...51M (https://ui.adsabs.harvard.edu/abs/2019Natur.566...51M). doi:10.1038/s41586-019-0897-9 (https://doi.org/10.1038%2Fs41586-019-0897-9). PMID 30728523 (https://pubmed.ncbi.nlm.nih.gov/30728523). S2CID 59606678 (https://api.semanticscholar.org/CorpusID:59606678).

37. Fitzpatrick, Mattias; Sundaresan, Neereja M.; Li, Andy C. Y.; Koch, Jens; Houck, Andrew A. (10 February 2017). "Observation of a Dissipative Phase Transition in a One-Dimensional Circuit QED Lattice". *Physical Review X*. **7** (1): 011016. arXiv:1607.06895 (https://arxiv.org/abs/1607.06895). Bibcode:2017PhRvX...7a1016F (https://ui.adsabs.harvard.edu/abs/2017PhRvX...7a1016F). doi:10.1103/PhysRevX.7.011016 (https://doi.org/10.1103%2FPhysRevX.7.011016). S2CID 3550701 (https://api.semanticscholar.org/CorpusID:3550701).

External links

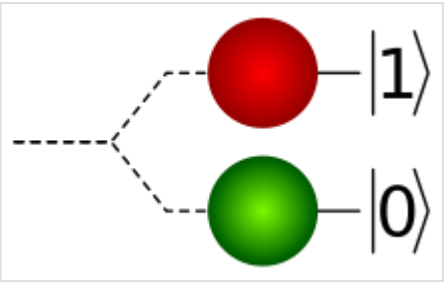
- Deutsch's 1985 paper (https://web.archive.org/web/20081123183419/http://www.ceid.upatras.gr/tech_news/papers/quantum_theory.pdf)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_simulator&oldid=1240080757"

WIKIPEDIA
The Free Encyclopedia

Qubit

In quantum computing, a **qubit** (/ˈkjuːbɪt/) or **quantum bit** is a basic unit of quantum information—the quantum version of the classic binary bit physically realized with a two-state device. A qubit is a two-state (or two-level) quantum-mechanical system, one of the simplest quantum systems displaying the peculiarity of quantum mechanics. Examples include the spin of the electron in which the two levels can be taken as spin up and spin down; or the polarization of a single photon in which the two spin states (left-handed and the right-handed circular polarization) can also be measured as horizontal and vertical linear polarization. In a classical system, a bit would have to be in one state or the other. However, quantum mechanics allows the qubit to be in a coherent superposition of multiple states simultaneously, a property that is fundamental to quantum mechanics and quantum computing.



The general definition of a qubit as the quantum state of a two-level quantum system.

Etymology

The coining of the term *qubit* is attributed to Benjamin Schumacher.[1] In the acknowledgments of his 1995 paper, Schumacher states that the term *qubit* was created in jest during a conversation with William Wootters.

Bit versus qubit

A binary digit, characterized as 0 or 1, is used to represent information in classical computers. When averaged over both of its states (0,1), a binary digit can represent up to one bit of Shannon information, where a bit is the basic unit of information. However, in this article, the word bit is synonymous with a binary digit.

In classical computer technologies, a *processed* bit is implemented by one of two levels of low DC voltage, and whilst switching from one of these two levels to the other, a so-called "forbidden zone" between two logic levels must be passed as fast as possible, as electrical voltage cannot change from one level to another instantaneously.

There are two possible outcomes for the measurement of a qubit—usually taken to have the value "0" and "1", like a bit. However, whereas the state of a bit can only be binary (either 0 or 1), the general state of a qubit according to quantum mechanics can arbitrarily be a coherent superposition of *all* computable states simultaneously.[2] Moreover, whereas a measurement of a classical bit would not disturb its state, a measurement of a qubit would destroy its coherence and irrevocably disturb the superposition state. It is possible to fully encode one bit in one qubit. However, a qubit can hold more information, e.g., up to two bits using superdense coding. Respectively, 8 qubits is called a *lnq*.

For a system of *n* components, a complete description of its state in classical physics requires only *n* bits, whereas in quantum physics a system of *n* qubits requires 2^n complex numbers (or a single point in a 2^n-dimensional vector space).[3]

Standard representation

In quantum mechanics, the general quantum state of a qubit can be represented by a linear superposition of its two orthonormal basis states (or basis vectors). These vectors are usually denoted as $|0\rangle = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $|1\rangle = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. They are written in the conventional Dirac—or "bra–ket"—notation; the $|0\rangle$ and $|1\rangle$ are pronounced "ket 0" and "ket 1", respectively. These two orthonormal basis states, $\{|0\rangle, |1\rangle\}$, together called the computational basis, are said to span the two-dimensional linear vector (Hilbert) space of the qubit.

Qubit basis states can also be combined to form product basis states. A set of qubits taken together is called a quantum register. For example, two qubits could be represented in a four-dimensional linear vector space spanned by the following product basis states:

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \text{ and } |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}.$$

In general, *n* qubits are represented by a superposition state vector in 2^n dimensional Hilbert space.

Qubit states

A pure qubit state is a coherent superposition of the basis states. This means that a single qubit (ψ) can be described by a linear combination of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are the probability amplitudes, and are both complex numbers. When we measure this qubit in the standard basis, according to the Born rule, the probability of outcome $|0\rangle$ with value "0" is $|\alpha|^2$ and the probability of outcome $|1\rangle$ with value "1" is $|\beta|^2$. Because the absolute squares of the amplitudes equate to probabilities, it follows that α and β must be constrained according to the second axiom of probability theory by the equation[5]

$$|\alpha|^2 + |\beta|^2 = 1.$$

The probability amplitudes, α and β, encode more than just the probabilities of the outcomes of a measurement; the *relative phase* between α and β is for example responsible for quantum interference, as seen in the double-slit experiment.

Bloch sphere representation

It might, at first sight, seem that there should be four degrees of freedom in $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, as α and β are complex numbers with two degrees of freedom each. However, one degree of freedom is removed by the normalization constraint $|\alpha|^2 + |\beta|^2 = 1$. This means, with a suitable change of coordinates, one can eliminate one of the degrees of freedom. One possible choice is that of Hopf coordinates:

$$\alpha = e^{i\delta} \cos\frac{\theta}{2},$$
$$\beta = e^{i(\delta+\varphi)} \sin\frac{\theta}{2}.$$

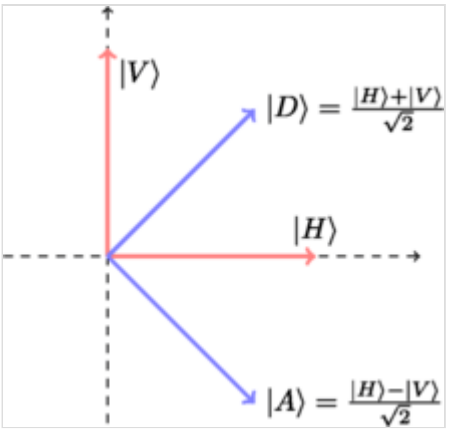
Additionally, for a single qubit the *global phase* of the state $e^{i\delta}$ has no physically observable consequences,[a] so we can arbitrarily choose α to be real (or β in the case that α is zero), leaving just two degrees of freedom:

$$\alpha = \cos\frac{\theta}{2},$$
$$\beta = e^{i\varphi} \sin\frac{\theta}{2},$$

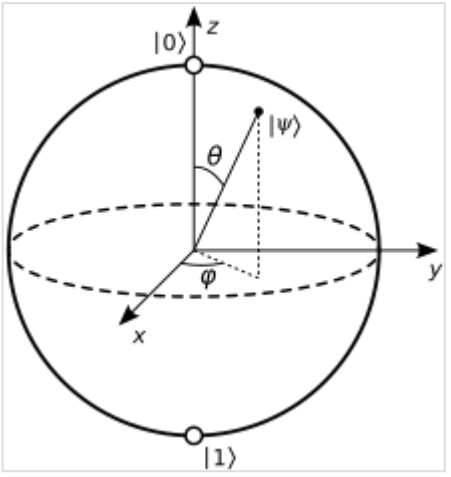
where $e^{i\varphi}$ is the physically significant *relative phase*.[6][b]

The possible quantum states for a single qubit can be visualised using a Bloch sphere (see picture). Represented on such a 2-sphere, a classical bit could only be at the "North Pole" or the "South Pole", in the locations where $|0\rangle$ and $|1\rangle$ are respectively. This particular choice of the polar axis is arbitrary, however. The rest of the surface of the Bloch sphere is inaccessible to a classical bit, but a pure qubit state can be represented by any point on the surface. For example, the pure qubit state $(|0\rangle + |1\rangle)/\sqrt{2}$ would lie on the equator of the sphere at the positive X-axis. In the classical limit, a qubit, which can have quantum states anywhere on the Bloch sphere, reduces to the classical bit, which can be found only at either poles.

The surface of the Bloch sphere is a two-dimensional space, which represents the observable state space of the pure qubit states. This state space has two local degrees of freedom, which can be represented by the two angles φ and θ.



Polarization of light offers a straightforward way to present orthogonal states. With a typical mapping $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$, quantum states $(|0\rangle \pm |1\rangle)/\sqrt{2}$ have a direct physical representation, both easily demonstrable experimentally in a class with linear polarizers and, for real α and β, matching the high-school definition of orthogonality.[4]



Bloch sphere representation of a qubit. The probability amplitudes for the superposition state, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, are given by $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\varphi}\sin\left(\frac{\theta}{2}\right)$

Mixed state

A pure state is fully specified by a single ket, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, a coherent superposition, represented by a point on the surface of the Bloch sphere as described above. Coherence is essential for a qubit to be in a superposition state. With interactions, quantum noise and decoherence, it is possible to put the qubit

in a mixed state, a statistical combination or "incoherent mixture" of different pure states. Mixed states can be represented by points *inside* the Bloch sphere (or in the Bloch ball). A mixed qubit state has three degrees of freedom: the angles φ and θ, as well as the length r of the vector that represents the mixed state.

Quantum error correction can be used to maintain the purity of qubits.

Operations on qubits

There are various kinds of physical operations that can be performed on qubits.

- Quantum logic gates, building blocks for a quantum circuit in a quantum computer, operate on a set of qubits (a register); mathematically, the qubits undergo a (reversible) unitary transformation described by multiplying the quantum gates unitary matrix with the quantum state vector. The result from this multiplication is a new quantum state.
- Quantum measurement is an irreversible operation in which information is gained about the state of a single qubit, and coherence is lost. The result of the measurement of a single qubit with the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ will be either $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$. Measurement of the state of the qubit alters the magnitudes of α and β. For instance, if the result of the measurement is $|1\rangle$, α is changed to 0 and β is changed to the phase factor $e^{i\phi}$ no longer experimentally accessible. If measurement is performed on a qubit that is entangled, the measurement may collapse the state of the other entangled qubits.
- Initialization or re-initialization to a known value, often $|0\rangle$. This operation collapses the quantum state (exactly like with measurement). Initialization to $|0\rangle$ may be implemented logically or physically: Logically as a measurement, followed by the application of the Pauli-X gate if the result from the measurement was $|1\rangle$. Physically, for example if it is a superconducting phase qubit, by lowering the energy of the quantum system to its ground state.
- Sending the qubit through a quantum channel to a remote system or machine (an I/O operation), potentially as part of a quantum network.

Quantum entanglement

An important distinguishing feature between qubits and classical bits is that multiple qubits can exhibit quantum entanglement; the qubit itself is an exhibition of quantum entanglement. In this case, quantum entanglement is a local or nonlocal property of two or more qubits that allows a set of qubits to express higher correlation than is possible in classical systems.

The simplest system to display quantum entanglement is the system of two qubits. Consider, for example, two entangled qubits in the $|\Phi^+\rangle$ Bell state:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

In this state, called an *equal superposition*, there are equal probabilities of measuring either product state $|00\rangle$ or $|11\rangle$, as $|1/\sqrt{2}|^2 = 1/2$. In other words, there is no way to tell if the first qubit has value "0" or "1" and likewise for the second qubit.

Imagine that these two entangled qubits are separated, with one each given to Alice and Bob. Alice makes a measurement of her qubit, obtaining—with equal probabilities—either $|0\rangle$ or $|1\rangle$, i.e., she can now tell if her qubit has value "0" or "1". Because of the qubits' entanglement, Bob must now get exactly the same measurement as Alice. For example, if she measures a $|0\rangle$, Bob must measure the same, as $|00\rangle$ is the only state where Alice's qubit is a $|0\rangle$. In short, for these two entangled qubits, whatever Alice measures, so would Bob, with perfect correlation, in any basis, however far apart they may be and even though both can not tell if their qubit has value "0" or "1" — a most surprising circumstance that cannot be explained by classical physics.

Controlled gate to construct the Bell state

Controlled gates act on 2 or more qubits, where one or more qubits act as a control for some specified operation. In particular, the controlled NOT gate (or CNOT or CX) acts on 2 qubits, and performs the NOT operation on the second qubit only when the first qubit is $|1\rangle$, and otherwise leaves it unchanged. With respect to the unentangled product basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, it maps the basis states as follows:

$$
\begin{aligned}
|00\rangle &\mapsto |00\rangle \\
|01\rangle &\mapsto |01\rangle \\
|10\rangle &\mapsto |11\rangle \\
|11\rangle &\mapsto |10\rangle .
\end{aligned}
$$

A common application of the CNOT gate is to maximally entangle two qubits into the $|\Phi^+\rangle$ Bell state. To construct $|\Phi^+\rangle$, the inputs A (control) and B (target) to the CNOT gate are:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_A \text{ and } |0\rangle_B$$

After applying CNOT, the output is the $|\Phi^+\rangle$ Bell State: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Applications

The $|\Phi^+\rangle$ Bell state forms part of the setup of the superdense coding, quantum teleportation, and entangled quantum cryptography algorithms.

Quantum entanglement also allows multiple states (such as the Bell state mentioned above) to be acted on simultaneously, unlike classical bits that can only have one value at a time. Entanglement is a necessary ingredient of any quantum computation that cannot be done efficiently on a classical computer. Many of the successes of quantum computation and communication, such as quantum teleportation and superdense coding, make use of entanglement, suggesting that entanglement is a resource that is unique to quantum

computation.[7] A major hurdle facing quantum computing, as of 2018, in its quest to surpass classical digital computing, is noise in quantum gates that limits the size of quantum circuits that can be executed reliably.[8]

Quantum register

A number of qubits taken together is a qubit register. Quantum computers perform calculations by manipulating qubits within a register.

Qudits and qutrits

The term **qudit** denotes the unit of quantum information that can be realized in suitable *d*-level quantum systems.[9] A qubit register that can be measured to *N* states is identical[c] to an *N*-level qudit. A rarely used[10] synonym for qudit is **quNit**,[11] since both *d* and *N* are frequently used to denote the dimension of a quantum system.

Qudits are similar to the integer types in classical computing, and may be mapped to (or realized by) arrays of qubits. Qudits where the *d*-level system is not an exponent of 2 cannot be mapped to arrays of qubits. It is for example possible to have 5-level qudits.

In 2017, scientists at the National Institute of Scientific Research constructed a pair of qudits with 10 different states each, giving more computational power than 6 qubits.[12]

In 2022, researchers at the University of Innsbruck succeeded in developing a universal qudit quantum processor with trapped ions.[13] In the same year, researchers at Tsinghua University's Center for Quantum Information implemented the dual-type qubit scheme in trapped ion quantum computers using the same ion species.[14]

Also in 2022, researchers at the University of California, Berkeley developed a technique to dynamically control the cross-Kerr interactions between fixed-frequency qutrits, achieving high two-qutrit gate fidelities.[15] This was followed by a demonstration of extensible control of superconducting qudits up to $\boldsymbol{d = 4}$ in 2024 based on programmable two-photon interactions.[16]

Similar to the qubit, the qutrit is the unit of quantum information that can be realized in suitable 3-level quantum systems. This is analogous to the unit of classical information trit of ternary computers.[17] Besides the advantage associated with the enlarged computational space, the third qutrit level can be exploited to implement efficient compilation of multi-qubit gates.[16][18][19]

Physical implementations

Any two-level quantum-mechanical system can be used as a qubit. Multilevel systems can be used as well, if they possess two states that can be effectively decoupled from the rest (e.g., the ground state and first excited state of a nonlinear oscillator). There are various proposals. Several physical implementations that approximate two-level systems to various degrees have been successfully realized.

Similarly to a classical bit where the state of a transistor in a processor, the magnetization of a surface in a hard disk and the presence of current in a cable can all be used to represent bits in the same computer, an eventual quantum computer is likely to use various combinations of qubits in its design.

All physical implementations are affected by noise. The so-called T_1 lifetime and T_2 dephasing time are a time to characterize the physical implementation and represent their sensitivity to noise. A higher time does not necessarily mean that one or the other qubit is better suited for quantum computing because gate times and fidelities need to be considered, too.

Different applications like Quantum sensing, Quantum computing and Quantum communication use different implementations of qubits to suit their application.

The following is an incomplete list of physical implementations of qubits, and the choices of basis are by convention only.

Physical support	Name	Information support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	Two electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Neutral atom	Atomic energy level	Spin	Up	Down
Trapped ion	Atomic energy level	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island (Q=0)	Charged superconducting island (Q=2e, one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up
Gapped topological system	Non-abelian anyons	Braiding of Excitations	Depends on specific topological system	Depends on specific topological system
Vibrational qubit[20]	Vibrational states	Phonon/vibron	$\|01\rangle$ superposition	$\|10\rangle$ superposition
van der Waals heterostructure[21]	Electron localization	Charge	Electron on bottom sheet	Electron on top sheet

Qubit storage

In 2008 a team of scientists from the U.K. and U.S. reported the first relatively long (1.75 seconds) and coherent transfer of a superposition state in an electron spin "processing" qubit to a nuclear spin "memory" qubit.[22] This event can be considered the first relatively consistent quantum data storage, a vital step towards the development of quantum computing. In 2013, a modification of similar systems (using charged rather than neutral donors) has dramatically extended this time, to 3 hours at very low temperatures and 39 minutes at room temperature.[23] Room temperature preparation of a qubit based on

electron spins instead of nuclear spin was also demonstrated by a team of scientists from Switzerland and Australia.[24] An increased coherence of qubits is being explored by researchers who are testing the limitations of a Ge hole spin-orbit qubit structure.[25]

See also

- Ancilla bit
- Bell state, W state and GHZ state
- Bloch sphere
- Electron-on-helium qubit
- Physical and logical qubits
- Quantum register
- Two-state quantum system
- The elements of the group U(2) are all possible single-qubit quantum gates[26]
- The circle group U(1) define the phase about the qubits basis states

Notes

a. This is because of the Born rule. The probability to observe an outcome upon measurement is the modulus squared of the probability amplitude for that outcome (or basis state, eigenstate). The *global phase* factor $e^{i\delta}$ is not measurable, because it applies to both basis states, and is on the complex unit circle so $|e^{i\delta}|^2 = 1$.
Note that by removing $e^{i\delta}$ it means that quantum states with global phase can not be represented as points on the surface of the Bloch sphere.

b. The Pauli Z basis is usually called the *computational basis*, where the relative phase have no effect on measurement. Measuring instead in the X or Y Pauli basis depends on the relative phase. For example, $(|0\rangle + e^{i\pi/2}|1\rangle)/\sqrt{2}$ will (because this state lies on the positive pole of the Y-axis) in the Y-basis always measure to the same value, while in the Z-basis results in equal probability of being measured to $|0\rangle$ or $|1\rangle$.
Because measurement collapses the quantum state, measuring the state in one basis hides some of the values that would have been measurable the other basis; See the uncertainty principle.

c. Actually isomorphic: For a register with n qubits $N = 2^n$ and $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^N$

References

1. B. Schumacher (1995). "Quantum coding". *Physical Review A*. **51** (4): 2738–2747. Bibcode:1995PhRvA..51.2738S (https://ui.adsabs.harvard.edu/abs/1995PhRvA..51.2738S). doi:10.1103/PhysRevA.51.2738 (https://doi.org/10.1103%2FPhysRevA.51.2738). PMID 9911903 (https://pubmed.ncbi.nlm.nih.gov/9911903).
2. Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press. p. 13 (https://archive.org/details/quantumcomputati00niel_993/page/n46). ISBN 978-1-107-00217-3.

3. Shor, Peter (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer∗". *SIAM Journal on Computing*. **26** (5): 1484–1509. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). Bibcode:1995quant.ph..8027S (https://ui.adsabs.harvard.edu/abs/1995quant.ph..8027S). doi:10.1137/S0097539795293172 (https://doi.org/10.1137%2FS0097539795293172). S2CID 2337707 (https://api.semanticscholar.org/CorpusID:2337707).
4. Seskir, Zeki C.; Migdał, Piotr; Weidner, Carrie; Anupam, Aditya; Case, Nicky; Davis, Noah; Decaroli, Chiara; Ercan, İlke; Foti, Caterina; Gora, Paweł; Jankiewicz, Klementyna; La Cour, Brian R.; Malo, Jorge Yago; Maniscalco, Sabrina; Naeemi, Azad; Nita, Laurentiu; Parvin, Nassim; Scafirimuto, Fabio; Sherson, Jacob F.; Surer, Elif; Wootton, James; Yeh, Lia; Zabello, Olga; Chiofalo, Marilù (2022). "Quantum games and interactive tools for quantum technologies outreach and education". *Optical Engineering*. **61** (8): 081809. arXiv:2202.07756 (https://arxiv.org/abs/2202.07756). Bibcode:2022OptEn..61h1809S (https://ui.adsabs.harvard.edu/abs/2022OptEn..61h1809S). doi:10.1117/1.OE.61.8.081809 (https://doi.org/10.1117%2F1.OE.61.8.081809). *This article incorporates text from this source, which is available under the CC BY 4.0 license.*
5. Colin P. Williams (2011). *Explorations in Quantum Computing*. Springer. pp. 9–13. ISBN 978-1-84628-887-6.
6. Nielsen, Michael A.; Chuang, Isaac (2010). *Quantum Computation and Quantum Information* (https://www.cambridge.org/9781107002173). Cambridge: Cambridge University Press. pp. 13–16. ISBN 978-1-10700-217-3. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
7. Horodecki, Ryszard; et al. (2009). "Quantum entanglement". *Reviews of Modern Physics*. **81** (2): 865–942. arXiv:quant-ph/0702225 (https://arxiv.org/abs/quant-ph/0702225). Bibcode:2009RvMP...81..865H (https://ui.adsabs.harvard.edu/abs/2009RvMP...81..865H). doi:10.1103/RevModPhys.81.865 (https://doi.org/10.1103%2FRevModPhys.81.865). S2CID 59577352 (https://api.semanticscholar.org/CorpusID:59577352).
8. Preskill, John (2018). "Quantum Computing in the NISQ era and beyond". *Quantum*. **2**: 79. arXiv:1801.00862 (https://arxiv.org/abs/1801.00862). Bibcode:2018Quant...2...79P (https://ui.adsabs.harvard.edu/abs/2018Quant...2...79P). doi:10.22331/q-2018-08-06-79 (https://doi.org/10.22331%2Fq-2018-08-06-79). S2CID 44098998 (https://api.semanticscholar.org/CorpusID:44098998).
9. Nisbet-Jones, Peter B. R.; Dilley, Jerome; Holleczek, Annemarie; Barter, Oliver; Kuhn, Axel (2013). "Photonic qubits, qutrits and ququads accurately prepared and delivered on demand" (http://stacks.iop.org/1367-2630/15/i=5/a=053007). *New Journal of Physics*. **15** (5): 053007. arXiv:1203.5614 (https://arxiv.org/abs/1203.5614). Bibcode:2013NJPh...15e3007N (https://ui.adsabs.harvard.edu/abs/2013NJPh...15e3007N). doi:10.1088/1367-2630/15/5/053007 (https://doi.org/10.1088%2F1367-2630%2F15%2F5%2F053007). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 110606655 (https://api.semanticscholar.org/CorpusID:110606655).
10. As of June 2022 1150 uses (https://arxiv.org/search/advanced?advanced=&terms-0-operator=AND&terms-0-term=qudit&terms-0-field=all&classification-physics=True&classification-physics_archives=quant-ph&classification-include_cross_list=include&date-filter_by=all_dates&date-year=&date-from_date=&date-to_date=&date-date_type=submitted_date&abstracts=show&size=50&order=-announced_date_first) versus 31 uses (https://arxiv.org/search/advanced?advanced=&terms-0-operator=AND&terms-0-term=qunit&terms-0-field=all&classification-physics=True&classification-physics_archives=quant-ph&classification-include_cross_list=include&date-filter_by=all_dates&date-year=&date-from_date=&date-to_date=&date-date_type=submitted_date&abstracts=show&size=50&order=-announced_date_first) on in the quant-ph category of arxiv.org.

11. Kaszlikowski, Dagomir; Gnaciński, Piotr; Żukowski, Marek; Miklaszewski, Wieslaw; Zeilinger, Anton (2000). "Violations of Local Realism by Two Entangled N-Dimensional Systems Are Stronger than for Two Qubits". *Phys. Rev. Lett*. **85** (21): 4418–4421. arXiv:quant-ph/0005028 (https://arxiv.org/abs/quant-ph/0005028). Bibcode:2000PhRvL..85.4418K (https://ui.adsabs.harvard.edu/abs/2000PhRvL..85.4418K). doi:10.1103/PhysRevLett.85.4418 (https://doi.org/10.1103%2FPhysRevLett.85.4418). PMID 11082560 (https://pubmed.ncbi.nlm.nih.gov/11082560). S2CID 39822693 (https://api.semanticscholar.org/CorpusID:39822693).
12. Choi, Charles Q. (2017-06-28). "Qudits: The Real Future of Quantum Computing?" (https://spectrum.ieee.org/qudits-the-real-future-of-quantum-computing). *IEEE Spectrum*. Retrieved 2017-06-29.
13. Ringbauer, Martin; Meth, Michael; Postler, Lukas; Stricker, Roman; Blatt, Rainer; Schindler, Philipp; Monz, Thomas (21 July 2022). "A universal qudit quantum processor with trapped ions" (https://www.nature.com/articles/s41567-022-01658-0). *Nature Physics*. **18** (9): 1053–1057. arXiv:2109.06903 (https://arxiv.org/abs/2109.06903). Bibcode:2022NatPh..18.1053R (https://ui.adsabs.harvard.edu/abs/2022NatPh..18.1053R). doi:10.1038/s41567-022-01658-0 (https://doi.org/10.1038%2Fs41567-022-01658-0). ISSN 1745-2481 (https://search.worldcat.org/issn/1745-2481). S2CID 237513730 (https://api.semanticscholar.org/CorpusID:237513730). Retrieved 21 July 2022.
14. Fardelli, Ingrid (August 18, 2022). "Researchers realize two coherently convertible qubit types using a single ion species" (https://phys.org/news/2022-08-coherently-qubit-ion-species.amp). Phys.org.
15. Goss, Noah; Morvan, Alexis; Marinelli, Brian; Mitchell, Bradley K.; Nguyen, Long B.; Naik, Ravi K.; Chen, Larry; Jünger, Christian; Kreikebaum, John Mark; Santiago, David I.; Wallman, Joel J.; Siddiqi, Irfan (2022-12-05). "High-fidelity qutrit entangling gates for superconducting circuits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9722686). *Nature Communications*. **13** (1). Springer Science and Business Media LLC: 7481. arXiv:2206.07216 (https://arxiv.org/abs/2206.07216). Bibcode:2022NatCo..13.7481G (https://ui.adsabs.harvard.edu/abs/2022NatCo..13.7481G). doi:10.1038/s41467-022-34851-z (https://doi.org/10.1038%2Fs41467-022-34851-z). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 9722686 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9722686). PMID 36470858 (https://pubmed.ncbi.nlm.nih.gov/36470858).
16. Nguyen, Long B.; Goss, Noah; Siva, Karthik; Kim, Yosep; Younis, Ed; Qing, Bingcheng; Hashim, Akel; Santiago, David I.; Siddiqi, Irfan (2024-08-19). "Empowering high-dimensional quantum computing by traversing the dual bosonic ladder" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11333499). *Nature Communications*. **15** (1). Springer Science and Business Media LLC: 7117. arXiv:2312.17741 (https://arxiv.org/abs/2312.17741). Bibcode:2024NatCo..15.7117N (https://ui.adsabs.harvard.edu/abs/2024NatCo..15.7117N). doi:10.1038/s41467-024-51434-2 (https://doi.org/10.1038%2Fs41467-024-51434-2). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 11333499 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11333499). PMID 39160166 (https://pubmed.ncbi.nlm.nih.gov/39160166).
17. Irving, Michael (2022-10-14). " "64-dimensional quantum space" drastically boosts quantum computing" (https://newatlas.com/telecommunications/qudits-64-dimensional-quantum-space/). *New Atlas*. Retrieved 2022-10-14.
18. Nguyen, L.B.; Kim, Y.; Hashim, A.; Goss, N.; Marinelli, B.; Bhandari, B.; Das, D.; Naik, R.K.; Kreikebaum, J.M.; Jordan, A.; Santiago, D.I.; Siddiqi, I. (16 January 2024). "Programmable Heisenberg interactions between Floquet qubits" (https://doi.org/10.1038%2Fs41567-023-02326-7). *Nature Physics*. **20** (1): 240–246. arXiv:2211.10383 (https://arxiv.org/abs/2211.10383). Bibcode:2024NatPh..20..240N (https://ui.adsabs.harvard.edu/abs/2024NatPh..20..240N). doi:10.1038/s41567-023-02326-7 (https://doi.org/10.1038%2Fs41567-023-02326-7).

19. Chu, Ji; He, Xiaoyu; Zhou, Yuxuan; Yuan, Jiahao; Zhang, Libo; Guo, Qihao; Hai, Yongju; Han, Zhikun; Hu, Chang-Kang; Huang, Wenhui; Jia, Hao; Jiao, Dawei; Li, Sai; Liu, Yang; Ni, Zhongchu; Nie, Lifu; Pan, Xianchuang; Qiu, Jiawei; Wei, Weiwei; Nuerbolati, Wuerkaixi; Yang, Zusheng; Zhang, Jiajian; Zhang, Zhida; Zou, Wanjing; Chen, Yuanzhen; Deng, Xiaowei; Deng, Xiuhao; Hu, Ling; Li, Jian; Liu, Song; Lu, Yao; Niu, Jingjing; Tan, Dian; Xu, Yuan; Yan, Tongxing; Zhong, Youpeng; Yan, Fei; Sun, Xiaoming; Yu, Dapeng (2022-11-14). "Scalable algorithm simplification using quantum AND logic". *Nature Physics*. **19** (1). Springer Science and Business Media LLC: 126–131. arXiv:2112.14922 (https://arxiv.org/abs/2112.14922). doi:10.1038/s41567-022-01813-7 (https://doi.org/10.1038%2Fs41567-022-01813-7). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473).
20. Eduardo Berrios; Martin Gruebele; Dmytro Shyshlov; Lei Wang; Dmitri Babikov (2012). "High fidelity quantum gates with vibrational qubits". *Journal of Chemical Physics*. **116** (46): 11347–11354. Bibcode:2012JPCA..11611347B (https://ui.adsabs.harvard.edu/abs/2012JPCA..11611347B). doi:10.1021/jp3055729 (https://doi.org/10.1021%2Fjp3055729). PMID 22803619 (https://pubmed.ncbi.nlm.nih.gov/22803619).
21. B. Lucatto; et al. (2019). "Charge qubit in van der Waals heterostructures". *Physical Review B*. **100** (12): 121406. arXiv:1904.10785 (https://arxiv.org/abs/1904.10785). Bibcode:2019PhRvB.100l1406L (https://ui.adsabs.harvard.edu/abs/2019PhRvB.100l1406L). doi:10.1103/PhysRevB.100.121406 (https://doi.org/10.1103%2FPhysRevB.100.121406). S2CID 129945636 (https://api.semanticscholar.org/CorpusID:129945636).
22. J. J. L. Morton; et al. (2008). "Solid-state quantum memory using the ^{31}P nuclear spin". *Nature*. **455** (7216): 1085–1088. arXiv:0803.2021 (https://arxiv.org/abs/0803.2021). Bibcode:2008Natur.455.1085M (https://ui.adsabs.harvard.edu/abs/2008Natur.455.1085M). doi:10.1038/nature07295 (https://doi.org/10.1038%2Fnature07295). S2CID 4389416 (https://api.semanticscholar.org/CorpusID:4389416).
23. Kamyar Saeedi; et al. (2013). "Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28". *Science*. **342** (6160): 830–833. arXiv:2303.17734 (https://arxiv.org/abs/2303.17734). Bibcode:2013Sci...342..830S (https://ui.adsabs.harvard.edu/abs/2013Sci...342..830S). doi:10.1126/science.1239584 (https://doi.org/10.1126%2Fscience.1239584). PMID 24233718 (https://pubmed.ncbi.nlm.nih.gov/24233718). S2CID 42906250 (https://api.semanticscholar.org/CorpusID:42906250).
24. Náfrádi, Bálint; Choucair, Mohammad; Dinse, Klaus-Pete; Forró, László (July 18, 2016). "Room temperature manipulation of long lifetime spins in metallic-like carbon nanospheres" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4960311). *Nature Communications*. **7**: 12232. arXiv:1611.07690 (https://arxiv.org/abs/1611.07690). Bibcode:2016NatCo...712232N (https://ui.adsabs.harvard.edu/abs/2016NatCo...712232N). doi:10.1038/ncomms12232 (https://doi.org/10.1038%2Fncomms12232). PMC 4960311 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4960311). PMID 27426851 (https://pubmed.ncbi.nlm.nih.gov/27426851).
25. Wang, Zhanning; Marcellina, Elizabeth; Hamilton, A. R.; Cullen, James H.; Rogge, Sven; Salfi, Joe; Culcer, Dimitrie (April 1, 2021). "Qubits composed of holes could be the trick to build faster, larger quantum computers" (https://phys.org/news/2021-04-qubits-holes-faster-larger-quantum.html). *npj Quantum Information*. **7** (1). arXiv:1911.11143 (https://arxiv.org/abs/1911.11143). doi:10.1038/s41534-021-00386-2 (https://doi.org/10.1038%2Fs41534-021-00386-2). S2CID 232486360 (https://api.semanticscholar.org/CorpusID:232486360).
26. Barenco, Adriano; Bennett, Charles H.; Cleve, Richard; DiVincenzo, David P.; Margolus, Norman; Shor, Peter; Sleator, Tycho; Smolin, John A.; Weinfurter, Harald (1995-11-01). "Elementary gates for quantum computation". *Physical Review A*. **52** (5). American Physical Society (APS): 3457–3467. arXiv:quant-ph/9503016 (https://arxiv.org/abs/quant-ph/9503016). Bibcode:1995PhRvA..52.3457B (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.3457B). doi:10.1103/physreva.52.3457 (https://doi.org/10.1103%2Fphysreva.52.3457). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). PMID 9912645 (https://pubmed.ncbi.nlm.nih.gov/9912645). S2CID 8764584 (https://api.semanticscholar.org/CorpusID:8764584).

Further reading

- Nielsen, Michael A.; Chuang, Isaac (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. ISBN 0521632358. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
- Colin P. Williams (2011). *Explorations in Quantum Computing*. Springer. ISBN 978-1-84628-887-6.
- Yanofsky, Noson S.; Mannucci, Mirco (2013). *Quantum computing for computer scientists*. Cambridge University Press. ISBN 978-0-521-87996-5.
- A treatment of two-level quantum systems, decades before the term "qubit" was coined, is found in the third volume of *The Feynman Lectures on Physics* (2013 ebook edition) (https://feynmanlectures.caltech.edu/III_toc.html), in chapters 9-11.
- A non-traditional motivation of the qubit aimed at non-physicists is found in *Quantum Computing Since Democritus*, by Scott Aaronson, Cambridge University Press (2013).
- An introduction to qubits for non-specialists, by the person who coined the word, is found in Lecture 21 of *The science of information: from language to black holes*, by Professor Benjamin Schumacher, The Great Courses, The Teaching Company (4DVDs, 2015).
- A picture book introduction to entanglement, showcasing a Bell state and the measurement of it, is found in *Quantum entanglement for babies*, by Chris Ferrie (2017). ISBN 9781492670261.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Qubit&oldid=1244266411"

WIKIPEDIA
The Free Encyclopedia

Physical and logical qubits

In quantum computing, a *qubit* is a unit of information analogous to a bit (binary digit) in classical computing, but it is affected by quantum mechanical properties such as superposition and entanglement which allow qubits to be in some ways more powerful than classical bits for some tasks. Qubits are used in quantum circuits and quantum algorithms composed of quantum logic gates to solve computational problems, where they are used for input/output and intermediate computations.

A **physical qubit** is a physical device that behaves as a two-state quantum system, used as a component of a computer system.[1][2] A **logical qubit** is a physical or abstract qubit that performs as specified in a quantum algorithm or quantum circuit[3] subject to unitary transformations, has a long enough coherence time to be usable by quantum logic gates (c.f. propagation delay for classical logic gates).[1][4][5]

Since the development of the first quantum computer in 1998, most technologies used to implement qubits face issues of stability, decoherence,[6][7] fault tolerance[8][9] and scalability.[6][9][10] Because of this, many physical qubits are needed for the purposes of error-correction to produce an entity which behaves logically as a single qubit would in a quantum circuit or algorithm; this is the subject of quantum error correction.[3][11] Thus, contemporary logical qubits typically consist of many physical qubits to provide stability, error-correction and fault tolerance needed to perform useful computations.[1][7][11]

In 2023, Google researchers showed how quantum error correction can improve logical qubit performance by increasing the physical qubit count.[12] These results found that a larger logical qubit (49 physical qubits) had a lower error rate, about 2.9 percent per round of error correction, compared to a rate of about 3.0 percent for the smaller logical qubit (17 physical qubits).[13]

In 2024, IBM researchers created a quantum error correction code 10 times more efficient than previous research, protecting 12 logical qubits for roughly a million cycles of error checks using 288 qubits.[14][15] The work demonstrates error correction on near-term devices while reducing overhead – the number of physical qubits required to keep errors low.[16]

In 2024, Microsoft and Quantinuum announced experimental results that showed logical qubits could be created with significantly fewer physical qubits.[17] The team used quantum error correction techniques developed by Microsoft and Quantinuum's trapped ion hardware to use 30 physical qubits to form four logical qubits. Scientists used a qubit virtualization system and active syndrome extraction—also called repeated error correction to accomplish this.[18] This work defines how to achieve logical qubits within quantum computation.[19]

Overview

1-bit and 2-bit quantum gate operations have been shown to be universal.[20][21][22][23] A quantum algorithm can be instantiated as a quantum circuit.[24][25]

A **logical** qubit specifies how a single qubit should behave in a quantum algorithm, subject to quantum logic operations which can be built out of quantum logic gates. However, issues in current technologies preclude single two-state quantum systems, which can be used as **physical** qubits, from reliably encoding and retaining this information for long enough to be useful. Therefore, current attempts to produce scalable quantum computers require quantum error correction, and multiple (currently many) physical qubits must be used to create a single, error-tolerant logical qubit. Depending on the error-correction scheme used, and the error rates of each physical qubit, a single logical qubit could be formed of up to 1,000 physical qubits.[26]

Topological quantum computing

The approach of topological qubits, which takes advantage of topological effects in quantum mechanics, has been proposed as needing many fewer or even a single physical qubit per logical qubit.[10] Topological qubits rely on a class of particles called anyons which have spin that is neither half-integral (fermions) nor integral (bosons), and therefore obey neither the Fermi–Dirac statistics nor the Bose–Einstein statistics of particle behavior.[27] Anyons exhibit braid symmetry in their world lines, which has desirable properties for the stability of qubits. Notably, anyons must exist in systems constrained to two spatial dimensions or fewer, according to the spin–statistics theorem, which states that in 3 or more spatial dimensions, only fermions and bosons are possible.[27]

See also

- Quantum error correction and the quantum threshold theorem
- Quantum computing § Obstacles
- Superconductive quantum computing
  - Josephson junction
- Trapped-ion quantum computing
- Semiconductor-based quantum computing
  - Quantum dot
- Topological quantum computing

References

1. Shaw, Bilal; Wilde, Mark M.; Oreshkov, Ognyan; Kremsky, Isaac; Lidar, Daniel A. (2008-07-18). "Encoding One Logical Qubit Into Six Physical Qubits". *Physical Review A*. **78** (1): 012337. arXiv:0803.1495 (https://arxiv.org/abs/0803.1495). Bibcode:2008PhRvA..78a2337S (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78a2337S). doi:10.1103/PhysRevA.78.012337 (https://doi.org/10.1103%2FPhysRevA.78.012337). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 40040752 (https://api.semanticscholar.org/CorpusID:40040752).

2. Viola, Lorenza; Knill, Emanuel; Laflamme, Raymond (2001-09-07). "Constructing Qubits in Physical Systems". *Journal of Physics A: Mathematical and General*. **34** (35): 7067–7079. arXiv:quant-ph/0101090 (https://arxiv.org/abs/quant-ph/0101090). Bibcode:2001JPhA...34.7067V (https://ui.adsabs.harvard.edu/abs/2001JPhA...34.7067V). doi:10.1088/0305-4470/34/35/331 (https://doi.org/10.1088%2F0305-4470%2F34%2F35%2F331). ISSN 0305-4470 (https://search.worldcat.org/issn/0305-4470). S2CID 14713492 (https://api.semanticscholar.org/CorpusID:14713492).
3. Heeres, Reinier W.; Reinhold, Philip; Ofek, Nissim; Frunzio, Luigi; Jiang, Liang; Devoret, Michel H.; Schoelkopf, Robert J. (2016-08-08). "Implementing a Universal Gate Set on a Logical Qubit Encoded in an Oscillator" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522494). *Nature Communications*. **8** (1): 94. arXiv:1608.02430 (https://arxiv.org/abs/1608.02430). doi:10.1038/s41467-017-00045-1 (https://doi.org/10.1038%2Fs41467-017-00045-1). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 5522494 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522494). PMID 28733580 (https://pubmed.ncbi.nlm.nih.gov/28733580).
4. "Logical Qubits (LogiQ)" (https://www.iarpa.gov/index.php/research-programs/logiq/logical-qubits). *Intelligence Advanced Research Projects Activity*. Retrieved 2018-09-18.
5. "Logical Qubits (LogiQ)" (https://www.iarpa.gov/index.php/research-programs/logiq/logical-qubits). *iarpa.gov*. Retrieved 2018-10-04.
6. Ristè, D.; Poletto, S.; Huang, M.-Z.; Bruno, A.; Vesterinen, V.; Saira, O.-P.; DiCarlo, L. (2014-10-20). "Detecting bit-flip errors in a logical qubit using stabilizer measurements" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4421804). *Nature Communications*. **6** (1): 6983. arXiv:1411.5542 (https://arxiv.org/abs/1411.5542). doi:10.1038/ncomms7983 (https://doi.org/10.1038%2Fncomms7983). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 4421804 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4421804). PMID 25923318 (https://pubmed.ncbi.nlm.nih.gov/25923318).
7. Kapit, Eliot (2016-04-12). "A Very Small Logical Qubit". *Physical Review Letters*. **116** (15): 150501. arXiv:1510.06117 (https://arxiv.org/abs/1510.06117). doi:10.1103/PhysRevLett.116.150501 (https://doi.org/10.1103%2FPhysRevLett.116.150501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 27127945 (https://pubmed.ncbi.nlm.nih.gov/27127945). S2CID 118476207 (https://api.semanticscholar.org/CorpusID:118476207).
8. Nigg, Daniel; Mueller, Markus; Martinez, Esteban A.; Schindler, Philipp; Hennrich, Markus; Monz, Thomas; Martin-Delgado, Miguel A.; Blatt, Rainer (2014-07-18). "Experimental Quantum Computations on a Topologically Encoded Qubit". *Science*. **345** (6194): 302–305. arXiv:1403.5426 (https://arxiv.org/abs/1403.5426). Bibcode:2014Sci...345..302N (https://ui.adsabs.harvard.edu/abs/2014Sci...345..302N). doi:10.1126/science.1253742 (https://doi.org/10.1126%2Fscience.1253742). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 24925911 (https://pubmed.ncbi.nlm.nih.gov/24925911). S2CID 9677048 (https://api.semanticscholar.org/CorpusID:9677048).
9. "Achieving scalability in quantum computing" (https://cloudblogs.microsoft.com/quantum/2018/05/16/achieving-scalability-in-quantum-computing/). *Microsoft Cloud Blogs*. Microsoft. 2018-05-16. Retrieved 2018-09-18.
10. Mishmash, Ryan; Alicea, Jason (2017-08-16). "Topological qubits: Arriving in 2018?" (https://quantumfrontiers.com/2017/08/16/topological-qubits-arriving-in-2018/). *Quantum Frontiers*. Retrieved 2018-09-17.
11. Jones, Cody; Fogarty, Michael A.; Morello, Andrea; Gyure, Mark F.; Dzurak, Andrew S.; Ladd, Thaddeus D. (2018-06-01). "A logical qubit in a linear array of semiconductor quantum dots". *Physical Review X*. **8** (2): 021058. arXiv:1608.06335 (https://arxiv.org/abs/1608.06335). Bibcode:2018PhRvX...8b1058J (https://ui.adsabs.harvard.edu/abs/2018PhRvX...8b1058J). doi:10.1103/PhysRevX.8.021058 (https://doi.org/10.1103%2FPhysRevX.8.021058). ISSN 2160-3308 (https://search.worldcat.org/issn/2160-3308). S2CID 119108989 (https://api.semanticscholar.org/CorpusID:119108989).

12. Acharya, Rajeev (2023-02-22). "Suppressing quantum errors by scaling a surface code logical qubit" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9946823). *Nature*. **614** (7949): 676–681. arXiv:2207.06431 (https://arxiv.org/abs/2207.06431). Bibcode:2023Natur.614..676G (https://ui.adsabs.harvard.edu/abs/2023Natur.614..676G). doi:10.1038/s41586-022-05434-1 (https://doi.org/10.1038%2Fs41586-022-05434-1). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9946823 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9946823). PMID 36813892 (https://pubmed.ncbi.nlm.nih.gov/36813892).
13. Conover, Emily (2023-02-22). "Google's quantum computer reached an error-correcting milestone" (https://www.sciencenews.org/article/google-quantum-computer-sycamore-milestone). *ScienceNews*. Retrieved 2024-07-09.
14. Bravyi, Sergei (2024-03-27). "High-threshold and low-overhead fault-tolerant quantum memory" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10972743). *Nature*. **627** (8005): 778–782. arXiv:2308.07915 (https://arxiv.org/abs/2308.07915). Bibcode:2024Natur.627..778B (https://ui.adsabs.harvard.edu/abs/2024Natur.627..778B). doi:10.1038/s41586-024-07107-7 (https://doi.org/10.1038%2Fs41586-024-07107-7). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 10972743 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10972743). PMID 38538939 (https://pubmed.ncbi.nlm.nih.gov/38538939).
15. Swayne, Matt (2024-03-28). "IBM Reports 10 Times More Efficient Error-Correcting Method Brings Practical Quantum Computers Closer To Reality" (https://thequantuminsider.com/2024/03/28/ibm-reports-10-times-more-efficient-error-correcting-method-brings-practical-quantum-computers-closer-to-reality/). *The Quantum Insider*. Retrieved 2024-07-09.
16. Crane, Leah (2023-08-18). "IBM has just made error correction easier for quantum computers" (https://www.newscientist.com/article/2388191-ibm-has-just-made-error-correction-easier-for-quantum-computers/). *New Scientist*. Retrieved 2024-07-09.
17. Choi, Charles (2024-04-03). "Microsoft Tests New Path to Reliable Quantum Computers - 1,000 physical qubits for each logical one? Try a dozen, says Redmond" (https://spectrum.ieee.org/microsoft-quantum-computer-quantinuum). *IEEE Spectrum*. Retrieved 2024-07-09.
18. Timmer, John (2024-04-03). "Quantum error correction used to actually correct errors" (https://arstechnica.com/science/2024/04/quantum-error-correction-used-to-actually-correct-errors/). *Ars Technica*. Retrieved 2024-07-09.
19. Sutor, Bob (2024-04-05). "Quantum in Context: Microsoft & Quantinuum Create Real Logical Qubits" (https://futurumgroup.com/insights/quantum-in-context-microsoft-quantinuum-create-real-logical-qubits/). *The Futurum Group*. Retrieved 2024-07-09.
20. DiVincenzo, David P. (1995-02-01). "Two-bit gates are universal for quantum computation". *Physical Review A*. **51** (2): 1015–1022. arXiv:cond-mat/9407022 (https://arxiv.org/abs/cond-mat/9407022). Bibcode:1995PhRvA..51.1015D (https://ui.adsabs.harvard.edu/abs/1995PhRvA..51.1015D). doi:10.1103/PhysRevA.51.1015 (https://doi.org/10.1103%2FPhysRevA.51.1015). PMID 9911679 (https://pubmed.ncbi.nlm.nih.gov/9911679). S2CID 2317415 (https://api.semanticscholar.org/CorpusID:2317415).
21. Deutsch, David; Barenco, Adriano; Ekert, Artur (1995-06-08). "Universality in Quantum Computation". *Proceedings of the Royal Society of London A: Mathematical and Physical Sciences*. **449** (1937): 669–677. arXiv:quant-ph/9505018 (https://arxiv.org/abs/quant-ph/9505018). Bibcode:1995RSPSA.449..669D (https://ui.adsabs.harvard.edu/abs/1995RSPSA.449..669D). CiteSeerX 10.1.1.54.2646 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.54.2646). doi:10.1098/rspa.1995.0065 (https://doi.org/10.1098%2Frspa.1995.0065). ISSN 1471-2946 (https://search.worldcat.org/issn/1471-2946). S2CID 15088854 (https://api.semanticscholar.org/CorpusID:15088854).

22. Barenco, Adriano (1995-06-08). "A Universal Two-Bit Gate for Quantum Computation". *Proceedings of the Royal Society of London A: Mathematical and Physical Sciences*. **449** (1937): 679–683. arXiv:quant-ph/9505016 (https://arxiv.org/abs/quant-ph/9505016). Bibcode:1995RSPSA.449..679B (https://ui.adsabs.harvard.edu/abs/1995RSPSA.449..679B). doi:10.1098/rspa.1995.0066 (https://doi.org/10.1098%2Frspa.1995.0066). ISSN 1471-2946 (https://search.worldcat.org/issn/1471-2946). S2CID 119447556 (https://api.semanticscholar.org/CorpusID:119447556).
23. Lloyd, Seth (1995-07-10). "Almost Any Quantum Logic Gate is Universal". *Physical Review Letters*. **75** (2): 346–349. Bibcode:1995PhRvL..75..346L (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75..346L). doi:10.1103/PhysRevLett.75.346 (https://doi.org/10.1103%2FPhysRevLett.75.346). PMID 10059671 (https://pubmed.ncbi.nlm.nih.gov/10059671).
24. Yazdani, Maryam; Zamani, Morteza Saheb; Sedighi, Mehdi (2013-06-09). "A Quantum Physical Design Flow Using ILP and Graph Drawing". *Quantum Information Processing Journal*. **12** (10): 3239. arXiv:1306.2037 (https://arxiv.org/abs/1306.2037). Bibcode:2013QuIP...12.3239Y (https://ui.adsabs.harvard.edu/abs/2013QuIP...12.3239Y). doi:10.1007/s11128-013-0597-6 (https://doi.org/10.1007%2Fs11128-013-0597-6). S2CID 12195937 (https://api.semanticscholar.org/CorpusID:12195937).
25. Whitney, Mark; Isailovic, Nemanja; Patel, Yatish; Kubiatowicz, John (2007-04-02). "Automated Generation of Layout and Control for Quantum Circuits" (https://archive.org/details/arxiv-0704.0268). *ACM Computing Frontiers*. arXiv:0704.0268 (https://arxiv.org/abs/0704.0268).
26. Fowler, Austin G.; Mariantoni, Matteo; Martinis, John M.; Cleland, Andrew N. (2012). "Surface codes: Towards practical large-scale quantum computation". *Physical Review A*. **86** (3): 032324. arXiv:1208.0928 (https://arxiv.org/abs/1208.0928). Bibcode:2012PhRvA..86c2324F (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86c2324F). doi:10.1103/PhysRevA.86.032324 (https://doi.org/10.1103%2FPhysRevA.86.032324). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 119277773 (https://api.semanticscholar.org/CorpusID:119277773).
27. Wilczek, Frank (2018-02-27). "How 'Anyon' Particles Emerge From Quantum Knots | Quanta Magazine" (https://www.quantamagazine.org/how-anyon-particles-emerge-from-quantum-knots-20170228/). *Quanta Magazine*. Retrieved 2018-09-18.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Physical_and_logical_qubits&oldid=1233631936"

WIKIPEDIA
The Free Encyclopedia

List of quantum processors

This list contains quantum processors, also known as quantum processing units (QPUs). Some devices listed below have only been announced at press conferences so far, with no actual demonstrations or scientific publications characterizing the performance.

Quantum processors are difficult to compare due to the different architectures and approaches. Due to this, published qubit numbers do not reflect the performance levels of the processor. This is instead achieved through benchmarking metrics such as quantum volume, randomized benchmarking or circuit layer operations per second (CLOPS).[1]

Circuit-based quantum processors

These QPUs are based on the quantum circuit and quantum logic gate-based model of computing.

Manufacturer	Name/codename designation	Architecture	Layout	Fidelity (%)	Qubits (physical)	Release date	Quantum volume
Alpine Quantum Technologies	PINE System[2]	Trapped ion			24[3]	June 7, 2021	128[4]
Atom Computing	Phoenix	Neutral atoms in optical lattices			100[5]	August 10, 2021	
Atom Computing	N/A	Neutral atoms in optical lattices			1180[6][7]	October 2023	
Google	N/A	Superconducting	N/A	99.5[8]	20	2017	
Google	N/A	Superconducting	7×7 lattice	99.7[8]	49[9]	Q4 2017 (planned)	
Google	Bristlecone	Superconducting transmon	6×12 lattice	99 (readout) 99.9 (1 qubit) 99.4 (2 qubits)	72[10][11]	March 5, 2018	
Google	Sycamore	Superconducting transmon	9×6 lattice	N/A	53 effective (54 total)	2019	
IBM	IBM Q 5 Tenerife	Superconducting	bow tie	99.897 (average gate) 98.64 (readout)	5	2016[8]	
IBM	IBM Q 5 Yorktown	Superconducting	bow tie	99.545 (average gate) 94.2 (readout)	5		
IBM	IBM Q 14 Melbourne	Superconducting	N/A	99.735 (average gate) 97.13 (readout)	14		
IBM	IBM Q 16 Rüschlikon	Superconducting	2×8 lattice	99.779 (average gate) 94.24 (readout)	16[12]	May 17, 2017 (Retired: 26 September 2018)[13]	
IBM	IBM Q 17	Superconducting	N/A	N/A	17[12]	May 17, 2017	
IBM	IBM Q 20 Tokyo	Superconducting	5×4 lattice	99.812 (average gate) 93.21 (readout)	20[14]	November 10, 2017	
IBM	IBM Q 20 Austin	Superconducting	5×4 lattice	N/A	20	(Retired: 4 July 2018)[13]	
IBM	IBM Q 50 prototype	Superconducting transmon	N/A	N/A	50[14]		
IBM	IBM Q 53	Superconducting	N/A	N/A	53	October 2019	
IBM	IBM Eagle	Superconducting	N/A	N/A	127[15]	November 2021	
IBM	IBM Osprey[6][7]	Superconducting	N/A	N/A	433[15]	November 2022	
IBM	IBM Condor[16][6]	Superconducting	N/A	N/A	1121[15]	December 2023	
IBM	IBM Heron[16][6]	Superconducting	N/A	N/A	133	December 2023	
IBM	IBM Armonk[17]	Superconducting	Single Qubit	N/A	1	October 16, 2019	
IBM	IBM Ourense[17]	Superconducting	T	N/A	5	July 3, 2019	
IBM	IBM Vigo[17]	Superconducting	T	N/A	5	July 3, 2019	
IBM	IBM London[17]	Superconducting	T	N/A	5	September 13, 2019	
IBM	IBM Burlington[17]	Superconducting	T	N/A	5	September 13, 2019	
IBM	IBM Essex[17]	Superconducting	T	N/A	5	September 13, 2019	
IBM	IBM Athens[18]	Superconducting		N/A	5		32[19]
IBM	IBM Belem[18]	Superconducting	Falcon r4T[20]	N/A	5		16[20]
IBM	IBM Bogotá[18]	Superconducting	Falcon r4L[20]	N/A	5		32[20]
IBM	IBM Casablanca[18]	Superconducting	Falcon r4H[20]	N/A	7	(Retired – March 2022)	32[20]
IBM	IBM Dublin[18]	Superconducting		N/A	27		64
IBM	IBM Guadalupe[18]	Superconducting	Falcon r4P[20]	N/A	16		32[20]
IBM	IBM Kolkata	Superconducting		N/A	27		128
IBM	IBM Lima[18]	Superconducting	Falcon r4T[20]	N/A	5		8[20]
IBM	IBM Manhattan[18]	Superconducting		N/A	65		32[19]
IBM	IBM Montreal[18]	Superconducting	Falcon r4[20]	N/A	27		128[20]
IBM	IBM Mumbai[18]	Superconducting	Falcon r5.1[20]	N/A	27		128[20]

IBM	IBM Paris[18]	Superconducting		N/A	27		32[19]
IBM	IBM Quito[18]	Superconducting	Falcon r4T[20]	N/A	5		16[20]
IBM	IBM Rome[18]	Superconducting		N/A	5		32[19]
IBM	IBM Santiago[18]	Superconducting		N/A	5		32[19]
IBM	IBM Sydney[18]	Superconducting	Falcon r4[20]	N/A	27		32[20]
IBM	IBM Toronto[18]	Superconducting	Falcon r4[20]	N/A	27		32[20]
Intel	17-Qubit Superconducting Test Chip	Superconducting	40-pin cross gap	N/A	17[21][22]	October 10, 2017	
Intel	Tangle Lake	Superconducting	108-pin cross gap	N/A	49[23]	January 9, 2018	
Intel	Tunnel Falls	Semiconductor spin qubits			12[24]	June 15, 2023	
IonQ	Harmony	Trapped ion	All-to-All[20]		11[25]	2022	8[20]
IonQ	Aria	Trapped ion	All-to-All[20]		25[25]	2022	
IonQ	Forte	Trapped ion	32x1 chain[26] All-to-All[20]	99.98 (1 qubit) 98.5–99.3 (2 qubit)[26]	32[25]	2022	
IQM	-	Superconducting	Star	99.91 (1 qubit) 99.14 (2 qubits)	5[27]	November 30, 2021[28]	N/A
IQM	-	Superconducting	Square lattice	99.91 (1 qubit median) 99.944 (1 qubit max) 98.25 (2 qubits median) 99.1 (2 qubits max)	20	October 9, 2023[29]	16[30]
M Squared Lasers	Maxwell	Neutral atoms in optical lattices		99.5 (3-qubit gate), 99.1 (4-qubit gate)[31]	200[32]	November 2022	
Oxford Quantum Circuits	Lucy[33]	Superconducting			8	2022	
Oxford Quantum Circuits	OQC Toshiko[34]	Superconducting			32	2023	
Quandela	Ascella (https://cloud.quandela.com/)	Photonics	N/A	99.6 (1 qubit) 93.8 (2 qubits) 86.0 (3 qubits)	6[35]	2022[36]	
QuTech at TU Delft	Spin-2	Semiconductor spin qubits		99 (average gate) 85 (readout)[37]	2	2020	
QuTech at TU Delft	-	Semiconductor spin qubits			6[38]	September 2022	
QuTech at TU Delft	Starmon-5	Superconducting	X configuration	97 (readout)[39]	5	2020	
Quantinuum	H2[40]	Trapped ion	Racetrack, All-to-All	99.997 (1 qubit) 99.8 (2 qubit)	56[41] (earlier 32)	May 9, 2023	65,536[42]
Quantinuum	H1-1[43]	Trapped ion	15×15 (Circuit Size)	99.996 (1 qubit) 99.914 (2 qubit)	20	2022	1,048,576[44]
Quantinuum	H1-2 [43]	Trapped ion	All-to-All[20]	99.996 (1 qubit) 99.7 (2 qubit)	12	2022	4096[45]
Quantware	Soprano[46]	Superconducting		99.9 (single-qubit gates)	5	July 2021	
Quantware	Contralto[47]	Superconducting		99.9 (single-qubit gates)	25	March 7, 2022[48]	
Quantware	Tenor[49]	Superconducting			64	February 23, 2023	
Rigetti	Agave	Superconducting	N/A	96 (Single-qubit gates) 87 (Two-qubit gates)	8	June 4, 2018[50]	
Rigetti	Acorn	Superconducting transmon	N/A	98.63 (Single-qubit gates) 87.5 (Two-qubit gates)	19[51]	December 17, 2017	
Rigetti	Aspen-1	Superconducting	N/A	93.23 (Single-qubit gates) 90.84 (Two-qubit gates)	16	November 30, 2018[50]	
Rigetti	Aspen-4	Superconducting		99.88 (Single-qubit gates) 94.42 (Two-qubit gates)	13	March 10, 2019	

Rigetti	Aspen-7	Superconducting		99.23 (Single-qubit gates) 95.2 (Two-qubit gates)	28	November 15, 2019	
Rigetti	Aspen-8	Superconducting		99.22 (Single-qubit gates) 94.34 (Two-qubit gates)	31	May 5, 2020	
Rigetti	Aspen-9	Superconducting		99.39 (Single-qubit gates) 94.28 (Two-qubit gates)	32	February 6, 2021	
Rigetti	Aspen-10	Superconducting		99.37 (Single-qubit gates) 94.66 (Two-qubit gates)	32	November 4, 2021	
Rigetti	Aspen-11	Superconducting	Octagonal[20]	99.8 (Single-qubit gates) 92.7 (Two-qubit gates CZ) 91.0 (Two-qubit gates XY)	40	December 15, 2021	
Rigetti	Aspen-M-1	Superconducting transmon	Octagonal[20]	99.8 (Single-qubit gates) 93.7 (Two-qubit gates CZ) 94.6 (Two-qubit gates XY)	80	February 15, 2022	8[20]
Rigetti	Aspen-M-2	Superconducting transmon		99.8 (Single-qubit gates) 91.3 (Two-qubit gates CZ) 90.0 (Two-qubit gates XY)	80	August 1, 2022	
Rigetti	Aspen-M-3	Superconducting transmon	N/A	99.9 (Single-qubit gates) 94.7 (Two-qubit gates CZ) 95.1 (Two-qubit gates XY)	80[52]	December 2, 2022	
Rigetti	Ankaa-2	Superconducting transmon	N/A	98 (Two-qubit gates)	84[53]	December 20, 2023	
RIKEN	RIKEN[54]	Superconducting	N/A	N/A	53 effective (64 total)[55][56]	March 27, 2023	N/A
SaxonQ	Princess	Nitrogen-vacancy center			4[57]	June 26, 2024	
SpinQ	Triangulum	Nuclear magnetic resonance			3[58]	September 2021	
USTC	Jiuzhang	Photonics	N/A	N/A	76[59][60]	2020	
USTC	Zuchongzhi	Superconducting	N/A	N/A	62[61]	2020	
USTC	Zuchongzhi 2.1	Superconducting	lattice[62]	99.86 (Single-qubit gates) 99.41 (Two-qubit gates) 95.48 (Readout)	66[63]	2021	
Xanadu	Borealis[64]	Photonics (Continuous-variable)	N/A	N/A	216[64]	2022[64]	
Xanadu	X8 [65]	Photonics (Continuous-variable)	N/A	N/A	8	2020	
Xanadu	X12	Photonics (Continuous-variable)	N/A	N/A	12	2020[65]	
Xanadu	X24	Photonics (Continuous-variable)	N/A	N/A	24	2020[65]	
CAS	Xiaohong[66]	Superconducting	N/A	N/A	504[66]	2024	

Annealing quantum processors

These QPUs are based on quantum annealing, not to be confused with digital annealing.[67]

Manufacturer	Name/Codename /Designation	Architecture	Layout	Fidelity (%)	Qubits	Release date
D-Wave	D-Wave One (Rainier)	Superconducting	C_4 = Chimera(4,4,4)[68] = 4×4 $K_{4,4}$	N/A	128	May 11, 2011
D-Wave	D-Wave Two	Superconducting	C_8 = Chimera(8,8,4)[68] = 8×8 $K_{4,4}$	N/A	512	2013
D-Wave	D-Wave 2X	Superconducting	C_{12} = Chimera(12,12,4)[68] = 12×12 $K_{4,4}$	N/A	1152	2015
D-Wave	D-Wave 2000Q	Superconducting	C_{16} = Chimera(16,16,4)[68] = 16×16 $K_{4,4}$	N/A	2048	2017
D-Wave	D-Wave Advantage	Superconducting	Pegasus P_{16}[69]	N/A	5760	2020
D-Wave	D-Wave Advantage 2[70][71][72][73]	Superconducting[70][71]	Zephyr Z_{15}[73][74]	N/A	7000+[70][71][72][73][74]	Late 2024 either 2025[70][71][72][73][74]

Analog quantum processors

These QPUs are based on analog Hamiltonian simulation.

Manufacturer	Name/Codename/Designation	Architecture	Layout	Fidelity (%)	Qubits	Release date
QuEra	Aquila	Neutral atoms	N/A	N/A	256[75]	November 2022

See also

- Quantum programming
- Timeline of quantum computing and communication

References

1. Wack, Andrew; Paik, Hanhee; Javadi-Abhari, Ali; Jurcevic, Petar; Faro, Ismael; Gambetta, Jay M.; Johnson, Blake R. (29 Oct 2021). "A practical heuristic for finding graph minors". arXiv:2110.14108 (https://arxiv.org/abs/2110.14108) [quant-ph (https://arxiv.org/archive/quant-ph)].
2. "THE SYSTEM IS THE FIRST COMMERCIAL 19-INCH RACK-MOUNTED ROOM-TEMPERATURE QUANTUM COMPUTER" (https://www.aqt.eu/pine-system-19-rack-mounted-quantum-computer/). *AQT*. Retrieved 21 Feb 2023.
3. Pogorelov, I.; Feldker, T.; Et, al. (2021-06-07). "Compact Ion-Trap Quantum Computing Demonstrator". *PRX Quantum*. **2** (2): 020343. arXiv:2101.11390 (https://arxiv.org/abs/2101.11390). Bibcode:2021PRXQ....2b0343P (https://ui.adsabs.harvard.edu/abs/2021PRXQ....2b0343P). doi:10.1103/PRXQuantum.2.020343 (https://doi.org/10.1103%2FPRXQuantum.2.020343). S2CID 231719119 (https://api.semanticscholar.org/CorpusID:231719119).
4. "STATE OF QUANTUM COMPUTING IN EUROPE: AQT PUSHING PERFORMANCE WITH A QUANTUM VOLUME OF 128" (https://www.aqt.eu/aqt-pushing-performance-with-a-quantum-volume-of-128/). *AQT*. 8 February 2023. Retrieved 24 Feb 2023.
5. Barnes, Katrina; Battaglino, Peter; Et, al. (2022). "Assembly and coherent control of a register of nuclear spin qubits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9120523). *Nature Communications*. **13** (1): 2779. arXiv:2108.04790 (https://arxiv.org/abs/2108.04790). Bibcode:2022NatCo..13.2779B (https://ui.adsabs.harvard.edu/abs/2022NatCo..13.2779B). doi:10.1038/s41467-022-29977-z (https://doi.org/10.1038%2Fs41467-022-29977-z). PMC 9120523 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9120523). PMID 35589685 (https://pubmed.ncbi.nlm.nih.gov/35589685). S2CID 236965948 (https://api.semanticscholar.org/CorpusID:236965948).
6. Padavic-Callaghan, Karmela (December 9, 2023). "IBM unveils 1000-qubit computer". *New Scientist*. p. 13.
7. Wilkins, Alex (October 24, 2023). "Record-breaking quantum computer has more than 1000 qubits" (https://www.newscientist.com/article/2399246-record-breaking-quantum-computer-has-more-than-1000-qubits/). *New Scientist*. Retrieved 2024-01-01.
8. Lant, Karla (2017-06-23). "Google is Closer Than Ever to a Quantum Computer Breakthrough" (https://futurism.com/google-is-closer-than-ever-to-a-quantum-computer-breakthrough/). *Futurism*. Retrieved 2017-10-18.
9. Simonite, Tom (2017-04-21). "Google's New Chip Is a Stepping Stone to Quantum Computing Supremacy" (https://www.technologyreview.com/s/604242/googles-new-chip-is-a-stepping-stone-to-quantum-computing-supremacy/). *MIT Technology Review*. Retrieved 2017-10-18.
10. "A Preview of Bristlecone, Google's New Quantum Processor" (https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html), *Research* (World wide web log), Google, March 2018.
11. Greene, Tristan (2018-03-06). "Google reclaims quantum computer crown with 72 qubit processor" (https://thenextweb.com/artificial-intelligence/2018/03/06/google-reclaims-quantum-computer-crown-with-72-qubit-processor/). *The Next Web*. Retrieved 2018-06-27.
12. "IBM Builds Its Most Powerful Universal Quantum Computing Processors" (https://web.archive.org/web/20170522235145/http://www-03.ibm.com/press/us/en/pressrelease/52403.wss). *IBM*. 2017-05-17. Archived from the original (https://www-03.ibm.com/press/us/en/pressrelease/52403.wss) on May 22, 2017. Retrieved 2017-10-18.
13. "Quantum devices & simulators" (https://www.research.ibm.com/ibm-q/technology/devices/). *IBM Q*. 2018-06-05. Retrieved 2019-03-29.
14. "IBM Announces Advances to IBM Quantum Systems & Ecosystem" (https://web.archive.org/web/20171110173121/http://www-03.ibm.com/press/us/en/pressrelease/53374.wss). 10 November 2017. Archived from the original (https://www-03.ibm.com/press/us/en/pressrelease/53374.wss) on November 10, 2017. Retrieved 10 November 2017.

15. Brooks, Michael (January–February 2024). "Bring on the noise". *MIT Technology Review*. Vol. 127, no. 1. Cambridge, Massachusetts. p. 50.
16. "IBM's 'Condor' quantum computer has more than 1000 qubits" (https://www.newscientist.com/article/2405789-ibms-condor-quantum-computer-has-more-than-1000-qubits/). *New Scientist*. Retrieved 2023-12-21.
17. "IBM Q Experience" (https://quantum-computing.ibm.com/). *IBM Q Experience*. Retrieved 2020-01-04.
18. "IBM Quantum" (https://quantum-computing.ibm.com/). *IBM Quantum*. Retrieved 2023-06-18.
19. "IBM Blog" (https://admin01.prod.blogs.cis.ibm.net/blog/). *IBM Blog*. Retrieved 2023-06-18.
20. Pelofske, Elijah; Bärtschi, Andreas; Eidenbenz, Stephan (2022). "Quantum Volume in Practice: What Users Can Expect from NISQ Devices". *IEEE Transactions on Quantum Engineering*. **3**: 1–19. arXiv:2203.03816 (https://arxiv.org/abs/2203.03816). doi:10.1109/TQE.2022.3184764 (https://doi.org/10.1109%2FTQE.2022.3184764). ISSN 2689-1808 (https://search.worldcat.org/issn/2689-1808). S2CID 247315182 (https://api.semanticscholar.org/CorpusID:247315182).
21. "Intel Delivers 17-Qubit Superconducting Chip with Advanced Packaging to QuTech" (https://newsroom.intel.com/news/intel-delivers-17-qubit-superconducting-chip-advanced-packaging-qutech/). 2017-10-10. Retrieved 2017-10-18.
22. Novet, Jordan (2017-10-10). "Intel shows off its latest chip for quantum computing as it looks past Moore's Law" (https://www.cnbc.com/2017/10/10/intel-delivers-17-qubit-quantum-computing-chip-to-qutech.html). *CNBC*. Retrieved 2017-10-18.
23. "CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy" (https://spectrum.ieee.org/intels-49qubit-chip-aims-for-quantum-supremacy). 2018-01-09. Retrieved 2018-01-14.
24. "Intel's New Chip to Advance Silicon Spin Qubit Research for Quantum Computing" (https://www.intel.com/content/www/us/en/newsroom/news/quantum-computing-chip-to-advance-research.html). *Intel Newsroom*. Retrieved 2023-07-09.
25. "IonQ | Trapped Ion Quantum Computing" (https://ionq.com/). *IonQ*. Retrieved 2023-05-02.
26. Egan, Laird; Debroy, Dripto M.; Noel, Crystal; Risinger, Andrew; Zhu, Daiwei; Biswas, Debopriyo; Newman, Michael; Li, Muyuan; Brown, Kenneth R.; Cetina, Marko; Monroe, Christopher (2020). "Fault-Tolerant Operation of a Quantum Error-Correction Code". arXiv:2009.11482 (https://arxiv.org/abs/2009.11482) [quant-ph (https://arxiv.org/archive/quant-ph)].
27. "The Power of Co-Design, Hermanni Heimonen, IQM" (https://www.youtube.com/watch?v=dLlUIkIsFig). *Youtube*. 2022-12-08. Retrieved 2023-06-09.
28. "Finland's first 5-qubit quantum computer is now operational" (https://www.vttresearch.com/en/news-and-ideas/finlands-first-5-qubit-quantum-computer-now-operational). *VTTresearch.com*. 2022-12-08. Retrieved 2023-06-09.
29. "Finland launches a 20-qubit quantum computer – development towards more powerful quantum computers continues" (https://meetiqm.com/resources/press-releases/finland-launches-a-20-qubit-quantum-computer/). *meetiqm.com*. 2023-10-09.
30. "Finland Unveils Second Quantum Computer with 20 Qubits, Aims for 50-Qubit Device by 2024" (https://quantumzeitgeist.com/finland-unveils-second-quantum-computer-with-20-qubits-aims-for-50-qubit-device-by-2024/). *quantumzeitgeist.com*. 2023-10-10.
31. Pelegrí, G.; Daley, A. J.; Pritchard, J. D. (2022). "High-fidelity multiqubit Rydberg gates via two-photon adiabatic rapid passage". *Quantum Science and Technology*. **7** (4): 045020. arXiv:2112.13025 (https://arxiv.org/abs/2112.13025). Bibcode:2022QS&T....7d5020P (https://ui.adsabs.harvard.edu/abs/2022QS&T....7d5020P). doi:10.1088/2058-9565/ac823a (https://doi.org/10.1088%2F2058-9565%2Fac823a). S2CID 245502083 (https://api.semanticscholar.org/CorpusID:245502083).
32. "MAXWELL: NEUTRAL ATOM QUANTUM PROCESSOR" (https://www.m2lasers.com/quantum-datasheet.html?file=Maxwell_Explainer.pdf) (PDF). *M Squared*. Retrieved 12 April 2023.
33. "Lucy" (https://oxfordquantumcircuits.com/oqc-on-aws). *Oxford Quantum Circuits*. 30 November 2021. Retrieved 20 Feb 2023.
34. "OQC Toshiko" (https://oxfordquantumcircuits.com/toshiko-the-worlds-first-enterprise-ready-quantum-platform). *Oxford Quantum Circuits*. 24 November 2023. Retrieved 27 Nov 2023.
35. Pont, M.; Corrielli, G.; Fyrillas, A.; et, al. (2022-11-29). "High-fidelity generation of four-photon GHZ states on-chip". arXiv:2211.15626 (https://arxiv.org/abs/2211.15626) [quant-ph (https://arxiv.org/archive/quant-ph)].
36. "La puissance d'un ordinateur quantique testée en ligne (The power of a quantum computer tested online)" (https://www.lemonde.fr/sciences/article/2022/11/22/la-puissance-d-un-ordinateur-quantique-testee-en-ligne_6151063_1650684.html). *Le Monde.fr*. Le Monde. 22 November 2022.
37. "Spin-2" (https://www.quantum-inspire.com/backends/spin-2/). *Quantum Inspire*. Retrieved 5 May 2021.
38. "Six-qubit silicon quantum processor sets a record" (https://physicsworld.com/a/six-qubit-silicon-quantum-processor-sets-a-record/). *PhysicsWorld*. 19 October 2022. Retrieved 2023-07-09.
39. "Starmon-5" (https://www.quantum-inspire.com/backends/starmon-5). *Quantum Inspire*. Retrieved 4 May 2021.
40. "Quantinuum H2 Product Data Sheet" (https://assets.website-files.com/62b9d45fb3f64842a96c9686/6459acc9b999bb7fb526c4bf_Quantinuum%20H2%20Product%20Data%20Sheet.pdf) (PDF).
41. "Quantinuum's H-Series hits 56 physical qubits that are all-to-all connected, and departs the era of classical simulation" (https://www.quantinuum.com/news/quantinuums-h-series-hits-56-physical-qubits-that-are-all-to-all-connected-and-departs-the-era-of-classical-simulation). *www.quantinuum.com*. Retrieved 2024-06-06.
42. "Quantinuum | Hardware | System Model H2" (https://www.quantinuum.com/hardware/h2). *www.quantinuum.com*. Retrieved 2023-05-12.
43. "Quantinuum System Model H1 Product Data Sheet" (https://assets.website-files.com/62b9d45fb3f64842a96c9686/648c742dd3e744dfeeb7cd06_Quantinuum%20H1%20Product%20Data%20Sheet%20v5.4%2015Jun23.pdf) (PDF). *Quantinuum*. Retrieved 8 Jul 2023.
44. "Quantinuum extends its significant lead in quantum computing, achieving historic milestones for hardware fidelity and Quantum Volume" (https://www.quantinuum.com/news/quantinuum-extends-its-significant-lead-in-quantum-computing-achieving-historic-milestones-for-hardware-fidelity-and-quantum-volume). *www.quantinuum.com*. Retrieved 2024-04-17.
45. "Quantinuum Announces Quantum Volume 4096 Achievement" (https://www.quantinuum.com/news/quantum-volume-reaches-5-digits-for-the-first-time-5-perspectives-on-what-it-means-for-quantum-computing). *Quantinuum*. Retrieved 24 Feb 2023.
46. "Soprano specs" (https://www.quantware.eu/product/soprano). *Quantware*. Retrieved 1 Feb 2023.
47. "Contralto specs" (https://www.quantware.eu/product/contralto). *Quantware*. Retrieved 21 Feb 2023.
48. "QUANTWARE RELEASES 25-QUBIT CONTRALTO QPU" (https://www.quantware.eu/press/quantware-releases-25-qubit-contralto-qpu). *Quantware*. Retrieved 21 Feb 2023.
49. "Tenor specs" (https://www.quantware.eu/product/tenor). *Quantware*. Retrieved 26 Feb 2023.
50. "QPU" (https://web.archive.org/web/20190516231438/https://www.rigetti.com/qpu). *Rigetti Computing*. Archived from the original (https://rigetti.com/qpu) on 2019-05-16. Retrieved 2019-03-24.
51. "Unsupervised Machine Learning on Rigetti 19Q with Forest 1.2" (https://medium.com/rigetti/unsupervised-machine-learning-on-rigetti-19q-with-forest-1-2-39021339699). 2017-12-18. Retrieved 2018-03-21.
52. "Aspen-M-3 Quantum Processor" (https://qcs.rigetti.com/qpus). Retrieved 2023-02-20.
53. Rigetti & Company LLC (2024-01-04). "Rigetti Announces Public Availability of Ankaa-2 System with a 2.5x Performance Improvement Compared to Previous QPUs" (https://www.globenewswire.com/news-release/2024/01/04/2804006/0/en/Rigetti-Announces-Public-Availability-of-Ankaa-2-System-with-a-2-5x-Performance-Improvement-Compared-to-Previous-QPUs.html). *GlobeNewswire News Room* (Press release). Retrieved 2024-01-23.
54. "Japan's first homemade quantum computer goes online" (https://www.riken.jp/en/news_pubs/news/2023/20230921_3/index.html). *www.riken.jp*. Retrieved 2024-01-25.

55. "Japanese joint research group launches quantum computing cloud service" (https://www.fujitsu.com/global/about/resources/news/press-releases/2023/0324-01.html). *Fujitsu Global*. Retrieved 2024-01-25.
56. "RIKEN and Fujitsu develop 64-qubit quantum computer" (https://www.riken.jp/en/news_pubs/news/2023/20231005_2/index.html). *www.riken.jp*. Retrieved 2024-01-25.
57. "All tests passed: DLR QCI accepts 4-qubit demonstrator SQ-RT with Princess QPU from SaxonQ" (https://qci.dlr.de/en/all-tests-passed-dlr-qci-accepts-4-qubit-demonstrator-sq-rt-with-princess-qpu-from-saxonq/). Retrieved 16 Jul 2024.
58. "Triangulum3 qubits desktop NMR quantum computer" (https://www.spinquanta.com/products-solutions/Triangulum). *AQT*. Retrieved 24 Feb 2023.
59. Ball, Philip (2020-12-03). "Physicists in China challenge Google's 'quantum advantage' " (https://doi.org/10.1038%2Fd41586-020-03434-7). *Nature*. **588** (7838): 380. Bibcode:2020Natur.588..380B (https://ui.adsabs.harvard.edu/abs/2020Natur.588..380B). doi:10.1038/d41586-020-03434-7 (https://doi.org/10.1038%2Fd41586-020-03434-7). PMID 33273711 (https://pubmed.ncbi.nlm.nih.gov/33273711).
60. Letzter, Rafi – Staff Writer 07 (7 December 2020). "China claims fastest quantum computer in the world" (https://www.livescience.com/china-quantum-supremacy.html). *livescience.com*. Retrieved 2020-12-19.
61. Ball, Philip (2020-12-03). "Strong Quantum Computational Advantage Using a Superconducting Quantum Processor". *Physical Review Letters*. **127** (18): 180501. arXiv:2106.14734 (https://arxiv.org/abs/2106.14734). Bibcode:2021PhRvL.127r0501W (https://ui.adsabs.harvard.edu/abs/2021PhRvL.127r0501W). doi:10.1103/PhysRevLett.127.180501 (https://doi.org/10.1103%2FPhysRevLett.127.180501). PMID 34767433 (https://pubmed.ncbi.nlm.nih.gov/34767433). S2CID 235658633 (https://api.semanticscholar.org/CorpusID:235658633).
62. Zhu, Qingling; et al. (2021). "Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling". *Science Bulletin*. **67** (3): 240–245. arXiv:2109.03494 (https://arxiv.org/abs/2109.03494). doi:10.1016/j.scib.2021.10.017 (https://doi.org/10.1016%2Fj.scib.2021.10.017). PMID 36546072 (https://pubmed.ncbi.nlm.nih.gov/36546072). S2CID 237442167 (https://api.semanticscholar.org/CorpusID:237442167).
63. Wu, Yulin; Bao, Wan-Su; Cao, Sirui; Chen, Fusheng; Chen, Ming-Cheng; Chen, Xiawei; Chung, Tung-Hsun; Deng, Hui; Du, Yajie; Fan, Daojin; Gong, Ming; Guo, Cheng; Guo, Chu; Guo, Shaojun; Han, Lianchen (2021-10-25). "Strong Quantum Computational Advantage Using a Superconducting Quantum Processor" (https://link.aps.org/doi/10.1103/PhysRevLett.127.180501). *Physical Review Letters*. **127** (18): 180501. arXiv:2106.14734 (https://arxiv.org/abs/2106.14734). Bibcode:2021PhRvL.127r0501W (https://ui.adsabs.harvard.edu/abs/2021PhRvL.127r0501W). doi:10.1103/PhysRevLett.127.180501 (https://doi.org/10.1103%2FPhysRevLett.127.180501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 34767433 (https://pubmed.ncbi.nlm.nih.gov/34767433). S2CID 235658633 (https://api.semanticscholar.org/CorpusID:235658633).
64. Madsen, Lars S.; Laudenbach, Fabian; Askarani, Mohsen Falamarzi; Rortais, Fabien; Vincent, Trevor; Bulmer, Jacob F. F.; Miatto, Filippo M.; Neuhaus, Leonhard; Helt, Lukas G.; Collins, Matthew J.; Lita, Adriana E. (June 2022). "Quantum computational advantage with a programmable photonic processor" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9159949). *Nature*. **606** (7912): 75–81. Bibcode:2022Natur.606...75M (https://ui.adsabs.harvard.edu/abs/2022Natur.606...75M). doi:10.1038/s41586-022-04725-x (https://doi.org/10.1038%2Fs41586-022-04725-x). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9159949 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9159949). PMID 35650354 (https://pubmed.ncbi.nlm.nih.gov/35650354). S2CID 249276257 (https://api.semanticscholar.org/CorpusID:249276257).
65. "A new kind of quantum" (https://spie.org/news/photonics-focus/novdec-2020/a-new-kind-of-quantum). *spie.org*. Retrieved 2021-01-09.
66. "China launches 504-qubit quantum chip, open to global users" (https://www.chinadaily.com.cn/a/202404/26/WS662b15dfa31082fc043c431e.html). *www.chinadaily.com.cn/*.
67. "Digital Annealer – Quantum Computing Technology" (https://www.fujitsu.com/global/services/business-services/digital-annealer/). *Fujitsu*. Retrieved 12 April 2023.
68. Cai, Jun; Macready, Bill; Roy, Aidan (10 Jun 2014). "A practical heuristic for finding graph minors". arXiv:1406.2741 (https://arxiv.org/abs/1406.2741) [quant-ph (https://arxiv.org/archive/quant-ph)].
69. Boothby, Kelly; Bunyk, Paul; Raymond, Jack; Roy, Aidan (29 Feb 2020). "Next-Generation Topology of D-Wave Quantum Processors". arXiv:2003.00133 (https://arxiv.org/abs/2003.00133) [quant-ph (https://arxiv.org/archive/quant-ph)].
70. "D-Wave Announces 1,200+ Qubit Advantage2™ Prototype in New, Lower-Noise Fabrication Stack, Demonstrating 20x Faster Time-to-Solution on Important Class of Hard Optimization Problems" (https://www.dwavesys.com/company/newsroom/press-release/d-wave-announces-1-200-qubit-advantage2-prototype-in-new-lower-noise-fabrication-stack-demonstrating-20x-faster-time-to-solution-on-important-class-of-hard-optimization-problems/).
71. "D-Wave Announces Availability of 1,200+ Qubit Advantage2™ Prototype in the Leap™ Quantum Cloud Service, Making its Most Performant System Available to Customers Today" (https://www.dwavesys.com/company/newsroom/press-release/d-wave-announces-availability-of-1-200-qubit-advantage2-prototype/).
72. https://www.dwavesys.com/media/xvjpraig/clarity-roadmap_digital_v2.pdf
73. https://www.dwavesys.com/media/eixhdtpa/14-1063a-a_the_d-wave_advantage2_prototype-4.pdf
74. "Ahead of the Game: D-Wave Delivers Prototype of Next-Generation Advantage2 Annealing Quantum Computer" (https://www.dwavesys.com/company/newsroom/press-release/ahead-of-the-game-d-wave-delivers-prototype-of-next-generation-advantage2-annealing-quantum-computer/).
75. Lee, Jane (2 November 2022). "Boston-based quantum computer QuEra joins Amazon's cloud for public access". Reuters.

Retrieved from "https://en.wikipedia.org/w/index.php?title=List_of_quantum_processors&oldid=1242251754"

WIKIPEDIA
The Free Encyclopedia

Cloud-based quantum computing

Cloud-based quantum computing is the invocation of quantum emulators, simulators or processors through the cloud. Increasingly, cloud services are being looked on as the method for providing access to quantum processing. Quantum computers achieve their massive computing power by initiating quantum physics into processing power and when users are allowed access to these quantum-powered computers through the internet it is known as quantum computing within the cloud.

In 2016, IBM connected a small quantum computer to the cloud and it allows for simple programs to be built and executed on the cloud.[1] In early 2017, researchers from Rigetti Computing demonstrated the first programmable cloud access using the pyQuil Python library.[2] Many people from academic researchers and professors to schoolkids, have already built programs that run many different quantum algorithms using the program tools. Some consumers hoped to use the fast computing to model financial markets or to build more advanced AI systems. These use methods allow people outside a professional lab or institution to experience and learn more about such a phenomenal technology.[3]

Application

Cloud based quantum computing is used in several contexts:

- In teaching, teachers can use cloud-based quantum computing to help their students better understand quantum mechanics, as well as implement and test quantum algorithms.[4][5]
- In research, scientists can use cloud-based quantum resources to test quantum information theories,[6] perform experiments,[7] compare architectures,[8] amongst other things.
- In games, developers can use cloud-based quantum resources can create quantum games to introduce people to quantum concepts.[9]
- In digital transformation where terabytes of big data available to process and forecast valuable future outcomes.
- Used in cloud based quantum app development to build customized applications for small businesses.

Existing platforms

- qBraid Lab by qBraid [10] is a cloud-based platform for quantum computing. It provides software tools for researchers and developers in quantum, as well as access to quantum hardware. qBraid provides cloud based access to IBM and Amazon Braket devices including IBM, Xanadu, OQC, QuEra, Amazon Braket simulators, Rigetti, and IonQ as of August 2023. The cloud quantum computing platform comes with a free tier where unlimited hardware and simulator access is available with the purchase of credits.
- Quandela Cloud by Quandela is the first cloud-accessible European photonic quantum computer. The computer is interfaced using the Perceval scripting language, with tutorials and documentation available online for free.[11]
- Xanadu Quantum Cloud by Xanadu which consists of cloud-based access to three fully programmable photonic quantum computers.[12]

- Forest by Rigetti Computing, which consists of a tool suite for quantum computing. It includes a programming language,[13] development tools and example algorithms.
- LIQUi> by Microsoft, which is a software architecture and tool suite for quantum computing. It includes a programming language, example optimization and scheduling algorithms, and quantum simulators.
    - Q#, a quantum programming language by Microsoft on the .NET Framework seen as a successor to LIQUi|>.
- IBM Q Experience by IBM,[14] providing access to quantum hardware as well as HPC simulators. These can be accessed programmatically using the Python-based Qiskit framework, or via graphical interface with the IBM Q Experience GUI.[15] Both are based on the OpenQASM standard for representing quantum operations. There is also a tutorial and online community.[16] Currently available simulators and quantum devices are:
    - Multiple transmon qubit processors.[17] Those with 5 and 16 qubits are publicly accessible. Devices up to 65 qubits are available through the IBM Q Network.[18]
    - A 32 qubit cloud-based simulator. Software for locally hosted simulators are also provided as part of Qiskit.
- Quantum in the Cloud by The University of Bristol, which consists of a quantum simulator and a four qubit optical quantum system.[19]
- Quantum Playground by Google, which features a simulator with a simple interface, and a scripting language and 3D quantum state visualization.[20]
- Quantum in the Cloud by Tsinghua University. It is a four-qubit new quantum cloud experience based on nuclear magnetic resonance-NMRCloudQ.
- Quantum Inspire by Qutech is the first platform in Europe providing cloud-based quantum computing to two hardware chips. Next to a 5-qubit transmon processor, Quantum Inspire is the first platform in the world [21] to provide online access to a fully programmable 2-qubit electron spin quantum processor:
    - Spin-2 is a 2-qubit spin qubit quantum computer, hosting two single electron spin qubits in a double quantum dot in isotopically purified ^{28}Si.
    - Starmon-5 consists of five superconducting transmon qubits in an X configuration.

    Next to the quantum chips, the platform gives access to QX, a quantum emulator backend. Two instances of the QX emulator are available, emulating up to 26 qubits on a commodity cloud-based server and up to 31 qubits using one 'fat' nodes on Cartesius, the Dutch national supercomputer of SurfSara. Circuit based quantum algorithms can be created through a graphical user interface or through the Python-based Quantum Inspire SDK, providing a backend for the projectQ framework, the Qiskit framework. Quantum Inspire provides a knowledge base[22] with user guides and some example algorithms written in cQASM.
- Amazon Braket, as of November 2022, provides access to quantum computers built by IonQ, Rigetti, Xanadu, QuEra, and Oxford Quantum Circuits. D-Wave machines can be used via the AWS Marketplace. Braket also provides a quantum algorithm development environment and simulator.

- Forge by QC Ware, providing access to D-Wave hardware as well as Google and IBM simulators. The platform offers a 30-day free trial including one minute of quantum computing time.[23]

References

1. "IBM Q Experience" (https://web.archive.org/web/20190614131004/https://quantumexperience.ng.bluemix.net/qx/editor). *quantumexperience.ng.bluemix.net*. Archived from the original (https://quantumexperience.ng.bluemix.net/qx/editor) on 2019-06-14. Retrieved 2019-05-08.
2. "Rigetti Computing Software Demo:Forest" (https://www.youtube.com/watch?v=IpoASc18P5Q). *YouTube*. Retrieved 2021-02-03.
3. Chen, Xi; Cheng, Bin; Li, Zhaokai; Nie, Xinfang; Yu, Nengkun; Yung, Man-Hong; Peng, Xinhua (2018). "Experimental Cryptographic Verification for Near-Term Quantum Cloud Computing". arXiv:1808.07375 (https://arxiv.org/abs/1808.07375) [quant-ph (https://arxiv.org/archive/quant-ph)].
4. "Undergraduates on a cloud using IBM Quantum Experience" (https://uwaterloo.ca/institute-for-quantum-computing/news/undergraduates-cloud-using-ibm-quantum-experience). 9 June 2016.
5. Fedortchenko, Serguei (8 July 2016). "A quantum teleportation experiment for undergraduate students". arXiv:1607.02398 (https://arxiv.org/abs/1607.02398) [quant-ph (https://arxiv.org/archive/quant-ph)].
6. Alsina, Daniel; Latorre, José Ignacio (11 July 2016). "Experimental test of Mermin inequalities on a five-qubit quantum computer". *Physical Review A*. **94** (1): 012314. arXiv:1605.04220 (https://arxiv.org/abs/1605.04220). Bibcode:2016PhRvA..94a2314A (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94a2314A). doi:10.1103/PhysRevA.94.012314 (https://doi.org/10.1103%2FPhysRevA.94.012314). S2CID 119189277 (https://api.semanticscholar.org/CorpusID:119189277).
7. Devitt, Simon J. (29 September 2016). "Performing quantum computing experiments in the cloud". *Physical Review A*. **94** (3): 032329. arXiv:1605.05709 (https://arxiv.org/abs/1605.05709). Bibcode:2016PhRvA..94c2329D (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94c2329D). doi:10.1103/PhysRevA.94.032329 (https://doi.org/10.1103%2FPhysRevA.94.032329). S2CID 119217150 (https://api.semanticscholar.org/CorpusID:119217150).
8. Linke, Norbert M.; Maslov, Dmitri; Roetteler, Martin; Debnath, Shantanu; Figgatt, Caroline; Landsman, Kevin A.; Wright, Kenneth; Monroe, Christopher (28 March 2017). "Experimental comparison of two quantum computing architectures" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5380037). *Proceedings of the National Academy of Sciences*. **114** (13): 3305–3310. arXiv:1702.01852 (https://arxiv.org/abs/1702.01852). Bibcode:2017PNAS..114.3305L (https://ui.adsabs.harvard.edu/abs/2017PNAS..114.3305L). doi:10.1073/pnas.1618020114 (https://doi.org/10.1073%2Fpnas.1618020114). ISSN 0027-8424 (https://search.worldcat.org/issn/0027-8424). PMC 5380037 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5380037). PMID 28325879 (https://pubmed.ncbi.nlm.nih.gov/28325879).
9. Wootton, James (12 March 2017). "Why we need to make quantum games" (https://medium.com/@decodoku/why-we-need-to-make-quantum-games-6f8c7bc4ace7). Medium.
10. qbraid.com

11. Heurtel, Nicolas; Fyrillas, Andreas; de Gliniasty, Grégoire; Le Bihan, Raphaël; Malherbe, Sébastien; Pailhas, Marceau; Bertasi, Eric; Bourdoncle, Boris; Emeriau, Pierre-Emmanuel; Mezher, Rawad; Music, Luka; Belabas, Nadia; Valiron, Benoît; Senellart, Pascale; Mansfield, Shane; Senellart, Jean (February 21, 2023). "Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing" (https://quantum-journal.org/papers/q-2023-02-21-931/). *Quantum*. **7**: 931. arXiv:2204.00602 (https://arxiv.org/abs/2204.00602). Bibcode:2023Quant...7..931H (https://ui.adsabs.harvard.edu/abs/2023Quant...7..931H). doi:10.22331/q-2023-02-21-931 (https://doi.org/10.22331%2Fq-2023-02-21-931). S2CID 247922568 (https://api.semanticscholar.org/CorpusID:247922568).
12. Choi, Charles Q. (9 September 2020). "First Photonic Quantum Computer on the Cloud" (https://spectrum.ieee.org/photonic-quantum). *IEEE Spectrum*.
13. Smith, Robert S.; Curtis, Michael J.; Zeng, William J. (2016-08-10). "A Practical Quantum Instruction Set Architecture". arXiv:1608.03355 (https://arxiv.org/abs/1608.03355) [quant-ph (https://arxiv.org/archive/quant-ph)].
14. "IBM Q Homepage" (https://www.research.ibm.com/ibm-q/). 2 April 2009.
15. "IBM Quantum Experience" (https://www.research.ibm.com/ibm-q/qx/). 2 April 2009.
16. "IBM Q Experience tutorial" (https://quantumexperience.ng.bluemix.net/qx/tutorial).
17. "Quantum devices and simulators" (https://www.research.ibm.com/ibm-q/technology/devices/?cm_mc_uid=27686633981315361542542&cm_mc_sid_50200000=20960861537781640898). 2 April 2009.
18. "IBM Q Network" (https://www.research.ibm.com/ibm-q/network/). 2 April 2009.
19. "Quantum in the Cloud" (http://www.bristol.ac.uk/physics/research/quantum/engagement/qcloud/). *bristol.ac.uk*. Retrieved 2017-07-20.
20. "Quantum Computing Playground" (http://www.quantumplayground.net/#/home). *quantumplayground.net*. Retrieved 2017-07-20.
21. "QuTech Announces Quantum Inspire, Europe's First Public Quantum Computing Platform" (https://quantumcomputingreport.com/news/qutech-announces-quantum-inspire-europes-first-public-quantum-computing-platform/). *quantumcomputingreport.com*. 22 April 2020. Retrieved 2020-05-05.
22. "The basics of Quantum Computing" (https://www.quantum-inspire.com/kbase/introduction-to-quantum-computing). *Quantum Inspire*. Retrieved 15 Nov 2018.
23. Lardinois, Frederic. "QC Ware Forge will give developers access to quantum hardware and simulators across vendors" (https://techcrunch.com/2019/09/25/qc-ware-forge-will-give-developers-access-to-quantum-hardware-and-simulators-across-vendors/). *TechCrunch*. Retrieved 29 October 2019.

External links

- List of quantum tools on quantum computing report (https://quantumcomputingreport.com/resources/tools/)
- List of quantum computing simulators on quantiki (https://www.quantiki.org/wiki/list-qc-simulators)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cloud-based_quantum_computing&oldid=1237650650"

WIKIPEDIA
The Free Encyclopedia

Bell's theorem

Bell's theorem is a term encompassing a number of closely related results in physics, all of which determine that quantum mechanics is incompatible with local hidden-variable theories, given some basic assumptions about the nature of measurement. "Local" here refers to the principle of locality, the idea that a particle can only be influenced by its immediate surroundings, and that interactions mediated by physical fields cannot propagate faster than the speed of light. "Hidden variables" are supposed properties of quantum particles that are not included in quantum theory but nevertheless affect the outcome of experiments. In the words of physicist John Stewart Bell, for whom this family of results is named, "If [a hidden-variable theory] is local it will not agree with quantum mechanics, and if it agrees with quantum mechanics it will not be local."[1]

The first such result was introduced by Bell in 1964, building upon the Einstein–Podolsky–Rosen paradox, which had called attention to the phenomenon of quantum entanglement. Bell deduced that if measurements are performed independently on the two separated particles of an entangled pair, then the assumption that the outcomes depend upon hidden variables within each half implies a mathematical constraint on how the outcomes on the two measurements are correlated. Such a constraint would later be named a **Bell inequality**. Bell then showed that quantum physics predicts correlations that violate this inequality. Multiple variations on Bell's theorem were put forward in the following years, using different assumptions and obtaining different Bell (or "Bell-type") inequalities.

The first rudimentary experiment designed to test Bell's theorem was performed in 1972 by John Clauser and Stuart Freedman.[2] More advanced experiments, known collectively as *Bell tests*, have been performed many times since. Often, these experiments have had the goal of "closing loopholes", that is, ameliorating problems of experimental design or set-up that could in principle affect the validity of the findings of earlier Bell tests. Bell tests have consistently found that physical systems obey quantum mechanics and violate Bell inequalities; which is to say that the results of these experiments are incompatible with any local hidden-variable theory.[3][4]

The exact nature of the assumptions required to prove a Bell-type constraint on correlations has been debated by physicists and by philosophers. While the significance of Bell's theorem is not in doubt, its full implications for the interpretation of quantum mechanics remain unresolved.

Theorem

There are many variations on the basic idea, some employing stronger mathematical assumptions than others.[5] Significantly, Bell-type theorems do not refer to any particular theory of local hidden variables, but instead show that quantum physics violates general assumptions behind classical pictures of nature. The original theorem proved by Bell in 1964 is not the most amenable to experiment, and it is convenient to introduce the genre of Bell-type inequalities with a later example.[6]

Hypothetical characters Alice and Bob stand in widely separated locations. Their colleague Victor prepares a pair of particles and sends one to Alice and the other to Bob. When Alice receives her particle, she chooses to perform one of two possible measurements (perhaps by flipping a coin to decide which). Denote these measurements by A_0 and A_1. Both A_0 and A_1 are *binary* measurements: the result of A_0 is either $+1$ or -1, and likewise for A_1. When Bob receives his particle, he chooses one of two measurements, B_0 and B_1, which are also both binary.

Suppose that each measurement reveals a property that the particle already possessed. For instance, if Alice chooses to measure A_0 and obtains the result $+1$, then the particle she received carried a value of $+1$ for a property a_0.[note 1] Consider the combination

$$a_0 b_0 + a_0 b_1 + a_1 b_0 - a_1 b_1 = (a_0 + a_1) b_0 + (a_0 - a_1) b_1 \,.$$

Because both a_0 and a_1 take the values ± 1, then either $a_0 = a_1$ or $a_0 = -a_1$. In the former case, the quantity $(a_0 - a_1) b_1$ must equal 0, while in the latter case, $(a_0 + a_1) b_0 = 0$. So, one of the terms on the right-hand side of the above expression will vanish, and the other will equal ± 2. Consequently, if the experiment is repeated over many trials, with Victor preparing new pairs of particles, the absolute value of the average of the combination $a_0 b_0 + a_0 b_1 + a_1 b_0 - a_1 b_1$ across all the trials will be less than or equal to 2. No *single* trial can measure this quantity, because Alice and Bob can only choose one measurement each, but on the assumption that the underlying properties exist, the average value of the sum is just the sum of the averages for each term. Using angle brackets to denote averages

$$|\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \leq 2 \,.$$

This is a Bell inequality, specifically, the CHSH inequality.[6]:115 Its derivation here depends upon two assumptions: first, that the underlying physical properties $a_0, a_1, b_0,$ and b_1 exist independently of being observed or measured (sometimes called the assumption of *realism*); and second, that Alice's choice of action cannot influence Bob's result or vice versa (often called the assumption of *locality*).[6]:117

Quantum mechanics can violate the CHSH inequality, as follows. Victor prepares a pair of qubits which he describes by the Bell state

$$|\psi\rangle = \frac{|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle}{\sqrt{2}},$$

where $|0\rangle$ and $|1\rangle$ are the eigenstates of one of the Pauli matrices,

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Victor then passes the first qubit to Alice and the second to Bob. Alice and Bob's choices of possible measurements are also defined in terms of the Pauli matrices. Alice measures either of the two observables σ_z and σ_x:

$$A_0 = \sigma_z,\ A_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

and Bob measures either of the two observables

$$B_0 = -\frac{\sigma_x + \sigma_z}{\sqrt{2}},\ B_1 = \frac{\sigma_x - \sigma_z}{\sqrt{2}}.$$

Victor can calculate the quantum expectation values for pairs of these observables using the Born rule:

$$\langle A_0 \otimes B_0 \rangle = \frac{1}{\sqrt{2}}, \langle A_0 \otimes B_1 \rangle = \frac{1}{\sqrt{2}}, \langle A_1 \otimes B_0 \rangle = \frac{1}{\sqrt{2}}, \langle A_1 \otimes B_1 \rangle = -\frac{1}{\sqrt{2}}\,.$$

While only one of these four measurements can be made in a single trial of the experiment, the sum

$$\langle A_0 \otimes B_0 \rangle + \langle A_0 \otimes B_1 \rangle + \langle A_1 \otimes B_0 \rangle - \langle A_1 \otimes B_1 \rangle = 2\sqrt{2}$$

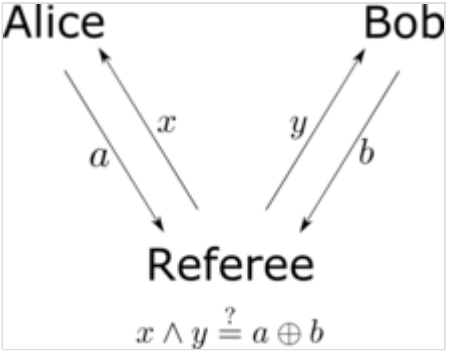
gives the sum of the average values that Victor expects to find across multiple trials. This value exceeds the classical upper bound of 2 that was deduced from the hypothesis of local hidden variables.[6]:116 The value $2\sqrt{2}$ is in fact the largest that quantum physics permits for this combination of expectation values, making it a Tsirelson bound.[9]:140

The CHSH inequality can also be thought of as a *game* in which Alice and Bob try to coordinate their actions.[10][11] Victor prepares two bits, x and y, independently and at random. He sends bit x to Alice and bit y to Bob. Alice and Bob win if they return answer bits a and b to Victor, satisfying

$$xy = a + b \mod 2\,.$$

Or, equivalently, Alice and Bob win if the logical AND of x and y is the logical XOR of a and b. Alice and Bob can agree upon any strategy they desire before the game, but they cannot communicate once the game begins. In any theory based on local hidden variables, Alice and Bob's probability of winning is no greater than $3/4$, regardless of what strategy they agree upon beforehand. However, if they share an entangled quantum state, their probability of winning can be as large as

$$\frac{2+\sqrt{2}}{4} \approx 0.85\,.$$



An illustration of the CHSH game: the referee, Victor, sends a bit each to Alice and to Bob, and Alice and Bob each send a bit back to the referee.

Variations and related results

Bell (1964)

Bell's 1964 paper points out that under restricted conditions, local hidden-variable models can reproduce the predictions of quantum mechanics. He then demonstrates that this cannot hold true in general.[12] Bell considers a refinement by David Bohm of the Einstein–Podolsky–Rosen (EPR) thought experiment. In this scenario, a pair of particles are formed together in such a way that they are described by a spin singlet state (which is an example of an entangled state). The particles then move apart in opposite directions. Each particle is measured by a Stern–Gerlach device, a measuring instrument that can be oriented in different directions and that reports one of two possible outcomes, representable by $+1$ and -1. The

configuration of each measuring instrument is represented by a unit vector, and the quantum-mechanical prediction for the correlation between two detectors with settings $\vec{a}$ and $\vec{b}$ is

$$P(\vec{a}, \vec{b}) = -\vec{a} \cdot \vec{b}.$$

In particular, if the orientation of the two detectors is the same ($\vec{a} = \vec{b}$), then the outcome of one measurement is certain to be the negative of the outcome of the other, giving $P(\vec{a}, \vec{a}) = -1$. And if the orientations of the two detectors are orthogonal ($\vec{a} \cdot \vec{b} = 0$), then the outcomes are uncorrelated, and $P(\vec{a}, \vec{b}) = 0$. Bell proves by example that these special cases *can* be explained in terms of hidden variables, then proceeds to show that the full range of possibilities involving intermediate angles *cannot*.

Bell posited that a local hidden-variable model for these correlations would explain them in terms of an integral over the possible values of some hidden parameter λ:

$$P(\vec{a}, \vec{b}) = \int d\lambda \, \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda),$$

where $\rho(\lambda)$ is a probability density function. The two functions $A(\vec{a}, \lambda)$ and $B(\vec{b}, \lambda)$ provide the responses of the two detectors given the orientation vectors and the hidden variable:

$$A(\vec{a}, \lambda) = \pm 1, \; B(\vec{b}, \lambda) = \pm 1.$$

Crucially, the outcome of detector A does not depend upon $\vec{b}$, and likewise the outcome of B does not depend upon $\vec{a}$, because the two detectors are physically separated. Now we suppose that the experimenter has a *choice* of settings for the second detector: it can be set either to $\vec{b}$ or to $\vec{c}$. Bell proves that the difference in correlation between these two choices of detector setting must satisfy the inequality

$$|P(\vec{a}, \vec{b}) - P(\vec{a}, \vec{c})| \leq 1 + P(\vec{b}, \vec{c}).$$

However, it is easy to find situations where quantum mechanics violates the Bell inequality.[13]:425–426 For example, let the vectors $\vec{a}$ and $\vec{b}$ be orthogonal, and let $\vec{c}$ lie in their plane at a 45° angle from both of them. Then

$$P(\vec{a}, \vec{b}) = 0,$$

while

$$P(\vec{a}, \vec{c}) = P(\vec{b}, \vec{c}) = -\frac{\sqrt{2}}{2},$$

but

$$\frac{\sqrt{2}}{2} \not\leq 1 - \frac{\sqrt{2}}{2}.$$

Therefore, there is no local hidden-variable model that can reproduce the predictions of quantum mechanics for all choices of $\vec{a}$, $\vec{b}$, and $\vec{c}$. Experimental results contradict the classical curves and match the curve predicted by quantum mechanics as long as experimental shortcomings are accounted for.[5]

Bell's 1964 theorem requires the possibility of perfect anti-correlations: the ability to make a probability-1 prediction about the result from the second detector, knowing the result from the first. This is related to the "EPR criterion of reality", a concept introduced in the 1935 paper by Einstein, Podolsky, and Rosen.

This paper posits: "If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of reality corresponding to that quantity."[14]

GHZ–Mermin (1990)

Daniel Greenberger, Michael A. Horne, and Anton Zeilinger presented a four-particle thought experiment in 1990, which David Mermin then simplified to use only three particles.[15][16] In this thought experiment, Victor generates a set of three spin-1/2 particles described by the quantum state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)\,,$$

where as above, $|0\rangle$ and $|1\rangle$ are the eigenvectors of the Pauli matrix σ_z. Victor then sends a particle each to Alice, Bob, and Charlie, who wait at widely separated locations. Alice measures either σ_x or σ_y on her particle, and so do Bob and Charlie. The result of each measurement is either $+1$ or -1. Applying the Born rule to the three-qubit state $|\psi\rangle$, Victor predicts that whenever the three measurements include one σ_x and two σ_y's, the product of the outcomes will always be $+1$. This follows because $|\psi\rangle$ is an eigenvector of $\sigma_x \otimes \sigma_y \otimes \sigma_y$ with eigenvalue $+1$, and likewise for $\sigma_y \otimes \sigma_x \otimes \sigma_y$ and $\sigma_y \otimes \sigma_y \otimes \sigma_x$. Therefore, knowing Alice's result for a σ_x measurement and Bob's result for a σ_y measurement, Victor can predict with probability 1 what result Charlie will return for a σ_y measurement. According to the EPR criterion of reality, there would be an "element of reality" corresponding to the outcome of a σ_y measurement upon Charlie's qubit. Indeed, this same logic applies to both measurements and all three qubits. Per the EPR criterion of reality, then, each particle contains an "instruction set" that determines the outcome of a σ_x or σ_y measurement upon it. The set of all three particles would then be described by the instruction set

$$(a_x, a_y, b_x, b_y, c_x, c_y)\,,$$

with each entry being either -1 or $+1$, and each σ_x or σ_y measurement simply returning the appropriate value.

If Alice, Bob, and Charlie all perform the σ_x measurement, then the product of their results would be $a_x b_x c_x$. This value can be deduced from

$$(a_x b_y c_y)(a_y b_x c_y)(a_y b_y c_x) = a_x b_x c_x a_y^2 b_y^2 c_y^2 = a_x b_x c_x\,,$$

because the square of either -1 or $+1$ is 1. Each factor in parentheses equals $+1$, so

$$a_x b_x c_x = +1\,,$$

and the product of Alice, Bob, and Charlie's results will be $+1$ with probability unity. But this is inconsistent with quantum physics: Victor can predict using the state $|\psi\rangle$ that the measurement $\sigma_x \otimes \sigma_x \otimes \sigma_x$ will instead yield -1 with probability unity.

This thought experiment can also be recast as a traditional Bell inequality or, equivalently, as a nonlocal game in the same spirit as the CHSH game.[17] In it, Alice, Bob, and Charlie receive bits x, y, z from Victor, promised to always have an even number of ones, that is, $x \oplus y \oplus z = 0$, and send him back bits a, b, c. They win the game if a, b, c have an odd number of ones for all inputs except $x = y = z = 0$,

when they need to have an even number of ones. That is, they win the game iff $a \oplus b \oplus c = x \vee y \vee z$. With local hidden variables the highest probability of victory they can have is 3/4, whereas using the quantum strategy above they win it with certainty. This is an example of quantum pseudo-telepathy.

Kochen–Specker theorem (1967)

In quantum theory, orthonormal bases for a Hilbert space represent measurements that can be performed upon a system having that Hilbert space. Each vector in a basis represents a possible outcome of that measurement.[note 2] Suppose that a hidden variable λ exists, so that knowing the value of λ would imply certainty about the outcome of any measurement. Given a value of λ, each measurement outcome – that is, each vector in the Hilbert space – is either *impossible* or *guaranteed*. A Kochen–Specker configuration is a finite set of vectors made of multiple interlocking bases, with the property that a vector in it will always be *impossible* when considered as belonging to one basis and *guaranteed* when taken as belonging to another. In other words, a Kochen–Specker configuration is an "uncolorable set" that demonstrates the inconsistency of assuming a hidden variable λ can be controlling the measurement outcomes.[22]:196–201

Free will theorem

The Kochen–Specker type of argument, using configurations of interlocking bases, can be combined with the idea of measuring entangled pairs that underlies Bell-type inequalities. This was noted beginning in the 1970s by Kochen,[23] Heywood and Redhead,[24] Stairs,[25] and Brown and Svetlichny.[26] As EPR pointed out, obtaining a measurement outcome on one half of an entangled pair implies certainty about the outcome of a corresponding measurement on the other half. The "EPR criterion of reality" posits that because the second half of the pair was not disturbed, that certainty must be due to a physical property belonging to it.[27] In other words, by this criterion, a hidden variable λ must exist within the second, as-yet unmeasured half of the pair. No contradiction arises if only one measurement on the first half is considered. However, if the observer has a choice of multiple possible measurements, and the vectors defining those measurements form a Kochen–Specker configuration, then some outcome on the second half will be simultaneously impossible and guaranteed.

This type of argument gained attention when an instance of it was advanced by John Conway and Simon Kochen under the name of the free will theorem.[28][29][30] The Conway–Kochen theorem uses a pair of entangled qutrits and a Kochen–Specker configuration discovered by Asher Peres.[31]

Quasiclassical entanglement

As Bell pointed out, some predictions of quantum mechanics can be replicated in local hidden-variable models, including special cases of correlations produced from entanglement. This topic has been studied systematically in the years since Bell's theorem. In 1989, Reinhard Werner introduced what are now called Werner states, joint quantum states for a pair of systems that yield EPR-type correlations but also admit a hidden-variable model.[32] Werner states are bipartite quantum states that are invariant under unitaries of symmetric tensor-product form:

$$\rho_{AB} = (U \otimes U)\rho_{AB}(U^\dagger \otimes U^\dagger).$$

In 2004, Robert Spekkens introduced a toy model that starts with the premise of local, discretized degrees of freedom and then imposes a "knowledge balance principle" that restricts how much an observer can

know about those degrees of freedom, thereby making them into hidden variables. The allowed states of knowledge ("epistemic states") about the underlying variables ("ontic states") mimic some features of quantum states. Correlations in the toy model can emulate some aspects of entanglement, like monogamy, but by construction, the toy model can never violate a Bell inequality.[33][34]

History

Background

The question of whether quantum mechanics can be "completed" by hidden variables dates to the early years of quantum theory. In his 1932 textbook on quantum mechanics, the Hungarian-born polymath John von Neumann presented what he claimed to be a proof that there could be no "hidden parameters". The validity and definitiveness of von Neumann's proof were questioned by Hans Reichenbach, in more detail by Grete Hermann, and possibly in conversation though not in print by Albert Einstein.[note 3] (Simon Kochen and Ernst Specker rejected von Neumann's key assumption as early as 1961, but did not publish a criticism of it until 1967.[40])

Einstein argued persistently that quantum mechanics could not be a complete theory. His preferred argument relied on a principle of locality:

> Consider a mechanical system constituted of two partial systems *A* and *B* which have interaction with each other only during limited time. Let the ψ function before their interaction be given. Then the Schrödinger equation will furnish the ψ function after their interaction has taken place. Let us now determine the physical condition of the partial system *A* as completely as possible by measurements. Then the quantum mechanics allows us to determine the ψ function of the partial system *B* from the measurements made, and from the ψ function of the total system. This determination, however, gives a result which depends upon *which* of the determining magnitudes specifying the condition of *A* has been measured (for instance coordinates *or* momenta). Since there can be only *one* physical condition of *B* after the interaction and which can reasonably not be considered as dependent on the particular measurement we perform on the system *A* separated from *B* it may be concluded that the ψ function is not unambiguously coordinated with the physical condition. This coordination of several ψ functions with the same physical condition of system *B* shows again that the ψ function cannot be interpreted as a (complete) description of a physical condition of a unit system.[41]

The EPR thought experiment is similar, also considering two separated systems *A* and *B* described by a joint wave function. However, the EPR paper adds the idea later known as the EPR criterion of reality, according to which the ability to predict with probability 1 the outcome of a measurement upon *B* implies the existence of an "element of reality" within *B*.[42]

In 1951, David Bohm proposed a variant of the EPR thought experiment in which the measurements have discrete ranges of possible outcomes, unlike the position and momentum measurements considered by EPR.[43] The year before, Chien-Shiung Wu and Irving Shaknov had successfully measured polarizations of photons produced in entangled pairs, thereby making the Bohm version of the EPR thought experiment practically feasible.[44]

By the late 1940s, the mathematician George Mackey had grown interested in the foundations of quantum physics, and in 1957 he drew up a list of postulates that he took to be a precise definition of quantum mechanics.[45] Mackey conjectured that one of the postulates was redundant, and shortly thereafter, Andrew M. Gleason proved that it was indeed deducible from the other postulates.[46][47] Gleason's theorem provided an argument that a broad class of hidden-variable theories are incompatible with quantum mechanics.[note 4] More specifically, Gleason's theorem rules out hidden-variable models that are "noncontextual". Any hidden-variable model for quantum mechanics must, in order to avoid the implications of Gleason's theorem, involve hidden variables that are not properties belonging to the measured system alone but also dependent upon the external context in which the measurement is made. This type of dependence is often seen as contrived or undesirable; in some settings, it is inconsistent with special relativity.[49][50] The Kochen–Specker theorem refines this statement by constructing a specific finite subset of rays on which no such probability measure can be defined.[49][51]

Tsung-Dao Lee came close to deriving Bell's theorem in 1960. He considered events where two kaons were produced traveling in opposite directions, and came to the conclusion that hidden variables could not explain the correlations that could be obtained in such situations. However, complications arose due to the fact that kaons decay, and he did not go so far as to deduce a Bell-type inequality.[36]:308

Bell's publications

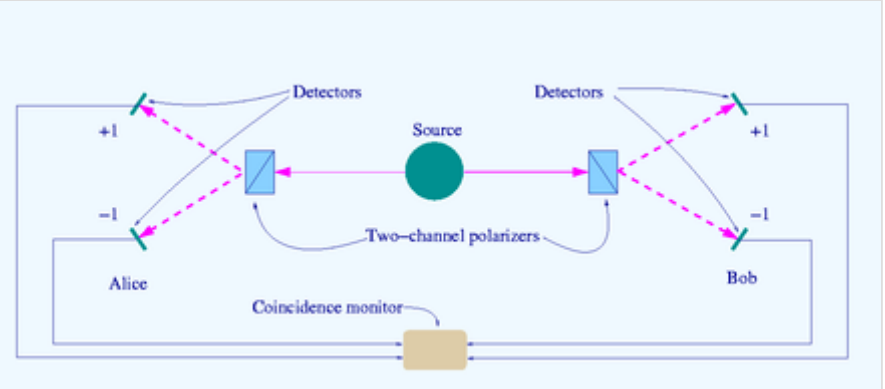
Bell chose to publish his theorem in a comparatively obscure journal because it did not require page charges, in fact paying the authors who published there at the time. Because the journal did not provide free reprints of articles for the authors to distribute, however, Bell had to spend the money he received to buy copies that he could send to other physicists.[52] While the articles printed in the journal themselves listed the publication's name simply as *Physics*, the covers carried the trilingual version *Physics Physique Физика* to reflect that it would print articles in English, French and Russian.[39]:92–100,289

Prior to proving his 1964 result, Bell also proved a result equivalent to the Kochen–Specker theorem (hence the latter is sometimes also known as the Bell–Kochen–Specker or Bell–KS theorem). However, publication of this theorem was inadvertently delayed until 1966.[49][53] In that paper, Bell argued that because an explanation of quantum phenomena in terms of hidden variables would require nonlocality, the EPR paradox "is resolved in the way which Einstein would have liked least."[53]

Experiments

In 1967, the unusual title *Physics Physique Физика* caught the attention of John Clauser, who then discovered Bell's paper and began to consider how to perform a Bell test in the laboratory.[54] Clauser and Stuart Freedman would go on to perform a Bell test in 1972.[55][56] This was only a limited test, because the choice of detector settings was made before the photons had left the source. In 1982, Alain Aspect and collaborators performed the first Bell test to remove this limitation.[57] This began a trend of progressively more stringent Bell tests. The GHZ thought experiment was implemented in practice, using entangled triplets of photons, in 2000.[58] By 2002, testing the CHSH inequality was feasible in undergraduate laboratory courses.[59]

In Bell tests, there may be problems of experimental design or set-up that affect the validity of the experimental findings. These problems are often referred to as "loopholes". The purpose of the experiment is to test whether nature can be described by local hidden-variable theory, which would contradict the predictions of quantum mechanics.



Scheme of a "two-channel" Bell test
The source S produces pairs of "photons", sent in opposite directions. Each photon encounters a two-channel polariser whose orientation (a or b) can be set by the experimenter. Emerging signals from each channel are detected and coincidences of four types (++, −−, +− and −+) counted by the coincidence monitor.

The most prevalent loopholes in real experiments are the *detection* and *locality* loopholes.[60] The detection loophole is opened when a small fraction of the particles (usually photons) are detected in the experiment, making it possible to explain the data with local hidden variables by assuming that the detected particles are an unrepresentative sample. The locality loophole is opened when the detections are not done with a spacelike separation, making it possible for the result of one measurement to influence the other without contradicting relativity. In some experiments there may be additional defects that make local-hidden-variable explanations of Bell test violations possible.[61]

Although both the locality and detection loopholes had been closed in different experiments, a long-standing challenge was to close both simultaneously in the same experiment. This was finally achieved in three experiments in 2015.[62][63][64][65][66] Regarding these results, Alain Aspect writes that "no experiment ... can be said to be totally loophole-free," but he says the experiments "remove the last doubts that we should renounce" local hidden variables, and refers to examples of remaining loopholes as being "far fetched" and "foreign to the usual way of reasoning in physics."[67]

These efforts to experimentally validate violations of the Bell inequalities would later result in Clauser, Aspect, and Anton Zeilinger being awarded the 2022 Nobel Prize in Physics.[68]

Interpretations

Reactions to Bell's theorem have been many and varied. Maximilian Schlosshauer, Johannes Kofler, and Zeilinger write that Bell inequalities provide "a wonderful example of how we can have a rigorous theoretical result tested by numerous experiments, and yet disagree about the implications."[69]

The Copenhagen interpretation

Copenhagen-type interpretations generally take the violation of Bell inequalities as grounds to reject the assumption often called counterfactual definiteness or "realism", which is not necessarily the same as abandoning realism in a broader philosophical sense.[70][71] For example, Roland Omnès argues for the rejection of hidden variables and concludes that "quantum mechanics is probably as realistic as any

theory of its scope and maturity ever will be".[72]:531 Likewise, Rudolf Peierls took the message of Bell's theorem to be that, because the premise of locality is physically reasonable, "hidden variables cannot be introduced without abandoning some of the results of quantum mechanics".[73][74]

This is also the route taken by interpretations that descend from the Copenhagen tradition, such as consistent histories (often advertised as "Copenhagen done right"),[75]:2839 as well as QBism.[76]

Many-worlds interpretation of quantum mechanics

The Many-worlds interpretation, also known as the Everett interpretation, is dynamically local, meaning that it does not call for action at a distance,[77]:17 and deterministic, because it consists of the unitary part of quantum mechanics without collapse. It can generate correlations that violate a Bell inequality because it violates an implicit assumption by Bell that measurements have a single outcome. In fact, Bell's theorem can be proven in the Many-Worlds framework from the assumption that a measurement has a single outcome. Therefore, a violation of a Bell inequality can be interpreted as a demonstration that measurements have multiple outcomes.[78]

The explanation it provides for the Bell correlations is that when Alice and Bob make their measurements, they split into local branches. From the point of view of each copy of Alice, there are multiple copies of Bob experiencing different results, so Bob cannot have a definite result, and the same is true from the point of view of each copy of Bob. They will obtain a mutually well-defined result only when their future light cones overlap. At this point we can say that the Bell correlation starts existing, but it was produced by a purely local mechanism. Therefore, the violation of a Bell inequality cannot be interpreted as a proof of non-locality.[77]:28

Non-local hidden variables

Most advocates of the hidden-variables idea believe that experiments have ruled out local hidden variables.[note 5] They are ready to give up locality, explaining the violation of Bell's inequality by means of a non-local hidden variable theory, in which the particles exchange information about their states. This is the basis of the Bohm interpretation of quantum mechanics, which requires that all particles in the universe be able to instantaneously exchange information with all others. One challenge for non-local hidden variable theories is to explain why this instantaneous communication can exist at the level of the hidden variables, but it cannot be used to send signals.[81] A 2007 experiment ruled out a large class of non-Bohmian non-local hidden variable theories, though not Bohmian mechanics itself.[82]

The transactional interpretation, which postulates waves traveling both backwards and forwards in time, is likewise non-local.[83]

Superdeterminism

A necessary assumption to derive Bell's theorem is that the hidden variables are not correlated with the measurement settings. This assumption has been justified on the grounds that the experimenter has "free will" to choose the settings, and that it is necessary to do science in the first place. A (hypothetical) theory where the choice of measurement is necessarily correlated with the system being measured is known as *superdeterministic*.[60]

A few advocates of deterministic models have not given up on local hidden variables. For example, Gerard 't Hooft has argued that superdeterminism cannot be dismissed.[84]

See also



- Einstein's thought experiments
- *Epistemological Letters*
- Fundamental Fysiks Group
- Leggett inequality
- Leggett–Garg inequality
- Mermin's device
- Mott problem
- PBR theorem
- Quantum contextuality
- Quantum nonlocality
- Renninger negative-result experiment

Notes

1. We are for convenience assuming that the response of the detector to the underlying property is deterministic. This assumption can be replaced; it is equivalent to postulating a joint probability distribution over all the observables of the experiment.[7][8]
2. In more detail, as developed by Paul Dirac,[18] David Hilbert,[19] John von Neumann,[20] and Hermann Weyl,[21] the state of a quantum mechanical system is a vector $|\psi\rangle$ belonging to a (separable) Hilbert space $\mathcal{H}$. Physical quantities of interest — position, momentum, energy, spin — are represented by "observables", which are self-adjoint linear operators acting on the Hilbert space. When an observable is measured, the result will be one of its eigenvalues with probability given by the Born rule: in the simplest case the eigenvalue η is non-degenerate and the probability is given by $|\langle\eta|\psi\rangle|^2$, where $|\eta\rangle$ is its associated eigenvector. More generally, the eigenvalue is degenerate and the probability is given by $\langle\psi|P_\eta\psi\rangle$, where P_η is the projector onto its associated eigenspace. For the purposes of this discussion, we can take the eigenvalues to be non-degenerate.
3. See Reichenbach[35] and Jammer,[36]:276 Mermin and Schack,[37] and for Einstein's remarks, Clauser and Shimony[38] and Wick.[39]:286
4. A hidden-variable theory that is deterministic implies that the probability of a given outcome is *always* either 0 or 1. For example, a Stern–Gerlach measurement on a spin-1 atom will report that the atom's angular momentum along the chosen axis is one of three possible values, which can be designated $-$, 0 and $+$. In a deterministic hidden-variable theory, there exists an underlying physical property that fixes the result found in the measurement. Conditional on the value of the underlying physical property, any given outcome (for example, a result of $+$) must be either impossible or guaranteed. But Gleason's theorem implies that there can be no such deterministic probability measure, because it proves that any probability measure must take the form of a mapping $u \to \langle \rho u, u\rangle$ for some density operator ρ. This mapping is continuous on the unit sphere of the Hilbert space, and since this unit sphere is connected, no continuous probability measure on it can be deterministic.[48]:§1.3

5. E. T. Jaynes was one exception,[79] but Jaynes' arguments have not generally been found persuasive.[80]

References

1. Bell, John S. (1987). *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press. p. 65. ISBN 9780521368698. OCLC 15053677 (https://search.worldcat.org/oclc/15053677).
2. "The Nobel Prize in Physics 2022" (https://www.nobelprize.org/prizes/physics/2022/press-release/). *Nobel Prize* (Press release). The Royal Swedish Academy of Sciences. October 4, 2022. Retrieved 6 October 2022.
3. The BIG Bell Test Collaboration (9 May 2018). "Challenging local realism with human choices". *Nature*. **557** (7704): 212–216. arXiv:1805.04431 (https://arxiv.org/abs/1805.04431). Bibcode:2018Natur.557..212B (https://ui.adsabs.harvard.edu/abs/2018Natur.557..212B). doi:10.1038/s41586-018-0085-3 (https://doi.org/10.1038%2Fs41586-018-0085-3). PMID 29743691 (https://pubmed.ncbi.nlm.nih.gov/29743691). S2CID 13665914 (https://api.semanticscholar.org/CorpusID:13665914).
4. Wolchover, Natalie (2017-02-07). "Experiment Reaffirms Quantum Weirdness" (https://www.quantamagazine.org/20170207-bell-test-quantum-loophole/). *Quanta Magazine*. Retrieved 2020-02-08.
5. Shimony, Abner. "Bell's Theorem" (https://plato.stanford.edu/entries/bell-theorem/). In Zalta, Edward N. (ed.). *Stanford Encyclopedia of Philosophy*.
6. Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information* (2nd ed.). Cambridge: Cambridge University Press. ISBN 978-1-107-00217-3. OCLC 844974180 (https://search.worldcat.org/oclc/844974180).
7. Fine, Arthur (1982-02-01). "Hidden Variables, Joint Probability, and the Bell Inequalities" (https://link.aps.org/doi/10.1103/PhysRevLett.48.291). *Physical Review Letters*. **48** (5): 291–295. Bibcode:1982PhRvL..48..291F (https://ui.adsabs.harvard.edu/abs/1982PhRvL..48..291F). doi:10.1103/PhysRevLett.48.291 (https://doi.org/10.1103%2FPhysRevLett.48.291). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007).
8. Braunstein, Samuel L.; Caves, Carlton M. (August 1990). "Wringing out better Bell inequalities". *Annals of Physics*. **202** (1): 22–56. Bibcode:1990AnPhy.202...22B (https://ui.adsabs.harvard.edu/abs/1990AnPhy.202...22B). doi:10.1016/0003-4916(90)90339-P (https://doi.org/10.1016%2F0003-4916%2890%2990339-P).
9. Rau, Jochen (2021). *Quantum theory : an information processing approach* (https://www.worldcat.org/oclc/1256446911). Oxford University Press. ISBN 978-0-192-65027-6. OCLC 1256446911 (https://search.worldcat.org/oclc/1256446911).
10. Cleve, R.; Hoyer, P.; Toner, B.; Watrous, J. (2004). "Consequences and limits of nonlocal strategies". *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004*. IEEE. pp. 236–249. arXiv:quant-ph/0404076 (https://arxiv.org/abs/quant-ph/0404076). Bibcode:2004quant.ph..4076C (https://ui.adsabs.harvard.edu/abs/2004quant.ph..4076C). doi:10.1109/CCC.2004.1313847 (https://doi.org/10.1109%2FCCC.2004.1313847). ISBN 0-7695-2120-7. OCLC 55954993 (https://search.worldcat.org/oclc/55954993). S2CID 8077237 (https://api.semanticscholar.org/CorpusID:8077237).

11. Barnum, H.; Beigi, S.; Boixo, S.; Elliott, M. B.; Wehner, S. (2010-04-06). "Local Quantum Measurement and No-Signaling Imply Quantum Correlations". *Physical Review Letters*. **104** (14): 140401. arXiv:0910.3952 (https://arxiv.org/abs/0910.3952). Bibcode:2010PhRvL.104n0401B (https://ui.adsabs.harvard.edu/abs/2010PhRvL.104n0401B). doi:10.1103/PhysRevLett.104.140401 (https://doi.org/10.1103%2FPhysRevLett.104.140401). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 20481921 (https://pubmed.ncbi.nlm.nih.gov/20481921). S2CID 17298392 (https://api.semanticscholar.org/CorpusID:17298392).
12. Bell, J. S. (1964). "On the Einstein Podolsky Rosen Paradox" (https://cds.cern.ch/record/111654/files/vol1p195-200_001.pdf) (PDF). *Physics Physique Физика*. **1** (3): 195–200. doi:10.1103/PhysicsPhysiqueFizika.1.195 (https://doi.org/10.1103%2FPhysicsPhysiqueFizika.1.195).
13. Griffiths, David J. (2005). *Introduction to Quantum Mechanics* (2nd ed.). Upper Saddle River, NJ: Pearson Prentice Hall. ISBN 0-13-111892-7. OCLC 53926857 (https://search.worldcat.org/oclc/53926857).
14. Einstein, A.; Podolsky, B.; Rosen, N. (1935-05-15). "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?" (https://doi.org/10.1103%2FPhysRev.47.777). *Physical Review*. **47** (10): 777–780. Bibcode:1935PhRv...47..777E (https://ui.adsabs.harvard.edu/abs/1935PhRv...47..777E). doi:10.1103/PhysRev.47.777 (https://doi.org/10.1103%2FPhysRev.47.777).
15. Greenberger, D.; Horne, M.; Shimony, A.; Zeilinger, A. (1990). "Bell's theorem without inequalities" (https://doi.org/10.1119%2F1.16243). *American Journal of Physics*. **58** (12): 1131. Bibcode:1990AmJPh..58.1131G (https://ui.adsabs.harvard.edu/abs/1990AmJPh..58.1131G). doi:10.1119/1.16243 (https://doi.org/10.1119%2F1.16243).
16. Mermin, N. David (1990). "Quantum mysteries revisited". *American Journal of Physics*. **58** (8): 731–734. Bibcode:1990AmJPh..58..731M (https://ui.adsabs.harvard.edu/abs/1990AmJPh..58..731M). doi:10.1119/1.16503 (https://doi.org/10.1119%2F1.16503).
17. Brassard, Gilles; Broadbent, Anne; Tapp, Alain (2005). "Recasting Mermin's multi-player game into the framework of pseudo-telepathy". *Quantum Information and Computation*. **5** (7): 538–550. arXiv:quant-ph/0408052 (https://arxiv.org/abs/quant-ph/0408052). Bibcode:2004quant.ph..8052B (https://ui.adsabs.harvard.edu/abs/2004quant.ph..8052B). doi:10.26421/QIC5.7-2 (https://doi.org/10.26421%2FQIC5.7-2).
18. Dirac, Paul Adrien Maurice (1930). *The Principles of Quantum Mechanics*. Oxford: Clarendon Press.
19. Hilbert, David (2009). Sauer, Tilman; Majer, Ulrich (eds.). *Lectures on the Foundations of Physics 1915–1927: Relativity, Quantum Theory and Epistemology*. Springer. doi:10.1007/b12915 (https://doi.org/10.1007%2Fb12915). ISBN 978-3-540-20606-4. OCLC 463777694 (https://search.worldcat.org/oclc/463777694).
20. von Neumann, John (1932). *Mathematische Grundlagen der Quantenmechanik*. Berlin: Springer. English translation: *Mathematical Foundations of Quantum Mechanics*. Translated by Beyer, Robert T. Princeton University Press. 1955.
21. Weyl, Hermann (1950) [1931]. *The Theory of Groups and Quantum Mechanics*. Translated by Robertson, H. P. Dover. ISBN 978-0-486-60269-1. Translated from the German *Gruppentheorie und Quantenmechanik* (2nd ed.). S. Hirzel Verlag. 1931.
22. Peres, Asher (1993). *Quantum Theory: Concepts and Methods*. Kluwer. ISBN 0-7923-2549-4. OCLC 28854083 (https://search.worldcat.org/oclc/28854083).
23. Redhead, Michael; Brown, Harvey (1991-07-01). "Nonlocality in Quantum Mechanics". *Proceedings of the Aristotelian Society, Supplementary Volumes*. **65** (1): 119–160. doi:10.1093/aristoteliansupp/65.1.119 (https://doi.org/10.1093%2Faristoteliansupp%2F65.1.119). ISSN 0309-7013 (https://search.worldcat.org/issn/0309-7013). JSTOR 4106773 (https://www.jstor.org/stable/4106773). "A similar approach was arrived at independently by Simon Kochen, although never published (private communication)."

24. Heywood, Peter; Redhead, Michael L. G. (May 1983). "Nonlocality and the Kochen–Specker paradox". *Foundations of Physics*. **13** (5): 481–499. Bibcode:1983FoPh...13..481H (https://ui.adsabs.harvard.edu/abs/1983FoPh...13..481H). doi:10.1007/BF00729511 (https://doi.org/10.1007%2FBF00729511). ISSN 0015-9018 (https://search.worldcat.org/issn/0015-9018). S2CID 120340929 (https://api.semanticscholar.org/CorpusID:120340929).
25. Stairs, Allen (December 1983). "Quantum Logic, Realism, and Value Definiteness". *Philosophy of Science*. **50** (4): 578–602. doi:10.1086/289140 (https://doi.org/10.1086%2F289140). ISSN 0031-8248 (https://search.worldcat.org/issn/0031-8248). S2CID 122885859 (https://api.semanticscholar.org/CorpusID:122885859).
26. Brown, H. R.; Svetlichny, G. (November 1990). "Nonlocality and Gleason's lemma. Part I. Deterministic theories". *Foundations of Physics*. **20** (11): 1379–1387. Bibcode:1990FoPh...20.1379B (https://ui.adsabs.harvard.edu/abs/1990FoPh...20.1379B). doi:10.1007/BF01883492 (https://doi.org/10.1007%2FBF01883492). ISSN 0015-9018 (https://search.worldcat.org/issn/0015-9018). S2CID 122868901 (https://api.semanticscholar.org/CorpusID:122868901).
27. Glick, David; Boge, Florian J. (2019-10-22). "Is the Reality Criterion Analytic?". *Erkenntnis*. **86** (6): 1445–1451. arXiv:1909.11893 (https://arxiv.org/abs/1909.11893). Bibcode:2019arXiv190911893G (https://ui.adsabs.harvard.edu/abs/2019arXiv190911893G). doi:10.1007/s10670-019-00163-w (https://doi.org/10.1007%2Fs10670-019-00163-w). ISSN 0165-0106 (https://search.worldcat.org/issn/0165-0106). S2CID 202889160 (https://api.semanticscholar.org/CorpusID:202889160).
28. Conway, John; Kochen, Simon (2006). "The Free Will Theorem". *Foundations of Physics*. **36** (10): 1441. arXiv:quant-ph/0604079 (https://arxiv.org/abs/quant-ph/0604079). Bibcode:2006FoPh...36.1441C (https://ui.adsabs.harvard.edu/abs/2006FoPh...36.1441C). doi:10.1007/s10701-006-9068-6 (https://doi.org/10.1007%2Fs10701-006-9068-6). S2CID 12999337 (https://api.semanticscholar.org/CorpusID:12999337).
29. Rehmeyer, Julie (2008-08-15). "Do subatomic particles have free will?" (https://www.sciencenews.org/article/do-subatomic-particles-have-free-will). *Science News*. Retrieved 2022-04-23.
30. Thomas, Rachel (2011-12-27). "John Conway – discovering free will (part I)" (https://plus.maths.org/content/john-conway-discovering-free-will-part-i). *Plus Magazine*. Retrieved 2022-04-23.
31. Conway, John H.; Kochen, Simon (2009). "The strong free will theorem" (http://www.ams.org/notices/200902/rtx090200226p.pdf) (PDF). *Notices of the AMS*. **56** (2): 226–232.
32. Werner, Reinhard F. (1989-10-01). "Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model". *Physical Review A*. **40** (8): 4277–4281. Bibcode:1989PhRvA..40.4277W (https://ui.adsabs.harvard.edu/abs/1989PhRvA..40.4277W). doi:10.1103/PhysRevA.40.4277 (https://doi.org/10.1103%2FPhysRevA.40.4277). ISSN 0556-2791 (https://search.worldcat.org/issn/0556-2791). PMID 9902666 (https://pubmed.ncbi.nlm.nih.gov/9902666).
33. Spekkens, Robert W. (2007-03-19). "Evidence for the epistemic view of quantum states: A toy theory". *Physical Review A*. **75** (3): 032110. arXiv:quant-ph/0401052 (https://arxiv.org/abs/quant-ph/0401052). Bibcode:2007PhRvA..75c2110S (https://ui.adsabs.harvard.edu/abs/2007PhRvA..75c2110S). doi:10.1103/PhysRevA.75.032110 (https://doi.org/10.1103%2FPhysRevA.75.032110). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 117284016 (https://api.semanticscholar.org/CorpusID:117284016).
34. Catani, Lorenzo; Browne, Dan E. (2017-07-27). "Spekkens' toy model in all dimensions and its relationship with stabiliser quantum mechanics" (https://doi.org/10.1088%2F1367-2630%2Faa781c). *New Journal of Physics*. **19** (7): 073035. arXiv:1701.07801 (https://arxiv.org/abs/1701.07801). Bibcode:2017NJPh...19g3035C (https://ui.adsabs.harvard.edu/abs/2017NJPh...19g3035C). doi:10.1088/1367-2630/aa781c (https://doi.org/10.1088%2F1367-2630%2Faa781c). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 119428107 (https://api.semanticscholar.org/CorpusID:119428107).

35. Reichenbach, Hans (1944). *Philosophic Foundations of Quantum Mechanics*. University of California Press. p. 14. OCLC 872622725 (https://search.worldcat.org/oclc/872622725).
36. Jammer, Max (1974). *The Philosophy of Quantum Mechanics*. John Wiley and Sons. ISBN 0-471-43958-4.
37. Mermin, N. David; Schack, Rüdiger (2018). "Homer nodded: von Neumann's surprising oversight". *Foundations of Physics*. **48** (9): 1007–1020. arXiv:1805.10311 (https://arxiv.org/abs/1805.10311). Bibcode:2018FoPh...48.1007M (https://ui.adsabs.harvard.edu/abs/2018FoPh...48.1007M). doi:10.1007/s10701-018-0197-5 (https://doi.org/10.1007%2Fs10701-018-0197-5). S2CID 118951033 (https://api.semanticscholar.org/CorpusID:118951033).
38. Clauser, J. F.; Shimony, A. (1978). "Bell's theorem: Experimental tests and implications" (http://www.physics.oregonstate.edu/~ostroveo/COURSES/ph651/Supplements_Phys651/RPP1978_Bell.pdf) (PDF). *Reports on Progress in Physics*. **41** (12): 1881–1927. Bibcode:1978RPPh...41.1881C (https://ui.adsabs.harvard.edu/abs/1978RPPh...41.1881C). CiteSeerX 10.1.1.482.4728 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.482.4728). doi:10.1088/0034-4885/41/12/002 (https://doi.org/10.1088%2F0034-4885%2F41%2F12%2F002). S2CID 250885175 (https://api.semanticscholar.org/CorpusID:250885175). Archived (https://web.archive.org/web/20170923004338/http://physics.oregonstate.edu/~ostroveo/COURSES/ph651/Supplements_Phys651/RPP1978_Bell.pdf) (PDF) from the original on 2017-09-23. Retrieved 2017-10-28.
39. Wick, David (1995). "Bell's Theorem". *The Infamous Boundary: Seven Decades of Heresy in Quantum Physics*. New York: Springer. pp. 92–100. doi:10.1007/978-1-4612-4030-3_11 (https://doi.org/10.1007%2F978-1-4612-4030-3_11). ISBN 978-0-387-94726-6.
40. Conway, John; Kochen, Simon (2002). "The Geometry of the Quantum Paradoxes". In Bertlmann, Reinhold A.; Zeilinger, Anton (eds.). *Quantum [Un]speakables: From Bell to Quantum Information*. Berlin: Springer. pp. 257–269. ISBN 3-540-42756-2. OCLC 49404213 (https://search.worldcat.org/oclc/49404213).
41. Einstein, Albert (March 1936). "Physics and reality". *Journal of the Franklin Institute*. **221** (3): 349–382. Bibcode:1936FrInJ.221..349E (https://ui.adsabs.harvard.edu/abs/1936FrInJ.221..349E). doi:10.1016/S0016-0032(36)91047-5 (https://doi.org/10.1016%2FS0016-0032%2836%2991047-5).
42. Harrigan, Nicholas; Spekkens, Robert W. (2010). "Einstein, incompleteness, and the epistemic view of quantum states". *Foundations of Physics*. **40** (2): 125. arXiv:0706.2661 (https://arxiv.org/abs/0706.2661). Bibcode:2010FoPh...40..125H (https://ui.adsabs.harvard.edu/abs/2010FoPh...40..125H). doi:10.1007/s10701-009-9347-0 (https://doi.org/10.1007%2Fs10701-009-9347-0). S2CID 32755624 (https://api.semanticscholar.org/CorpusID:32755624).
43. Bohm, David (1989) [1951]. *Quantum Theory* (Dover reprint ed.). Prentice-Hall. pp. 614–623. ISBN 978-0-486-65969-5. OCLC 1103789975 (https://search.worldcat.org/oclc/1103789975).
44. Wu, C.-S.; Shaknov, I. (1950). "The Angular Correlation of Scattered Annihilation Radiation". *Physical Review*. **77** (1): 136. Bibcode:1950PhRv...77..136W (https://ui.adsabs.harvard.edu/abs/1950PhRv...77..136W). doi:10.1103/PhysRev.77.136 (https://doi.org/10.1103%2FPhysRev.77.136).
45. Mackey, George W. (1957). "Quantum Mechanics and Hilbert Space". *The American Mathematical Monthly*. **64** (8P2): 45–57. doi:10.1080/00029890.1957.11989120 (https://doi.org/10.1080%2F00029890.1957.11989120). JSTOR 2308516 (https://www.jstor.org/stable/2308516).
46. Gleason, Andrew M. (1957). "Measures on the closed subspaces of a Hilbert space" (http://www.iumj.indiana.edu/IUMJ/FULLTEXT/1957/6/56050). *Indiana University Mathematics Journal*. **6** (4): 885–893. doi:10.1512/iumj.1957.6.56050 (https://doi.org/10.1512%2Fiumj.1957.6.56050). MR 0096113 (https://mathscinet.ams.org/mathscinet-getitem?mr=0096113).
47. Chernoff, Paul R. "Andy Gleason and Quantum Mechanics" (https://www.ams.org/notices/200910/rtx091001236p.pdf) (PDF). *Notices of the AMS*. **56** (10): 1253–1259.

48. Wilce, A. (2017). "Quantum Logic and Probability Theory" (https://plato.stanford.edu/entries/qt-quantlog/). *Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University.
49. Mermin, N. David (July 1993). "Hidden Variables and the Two Theorems of John Bell" (http://cqi.inf.usi.ch/qic/Mermin1993.pdf) (PDF). *Reviews of Modern Physics*. **65** (3): 803–815. arXiv:1802.10119 (https://arxiv.org/abs/1802.10119). Bibcode:1993RvMP...65..803M (https://ui.adsabs.harvard.edu/abs/1993RvMP...65..803M). doi:10.1103/RevModPhys.65.803 (https://doi.org/10.1103%2FRevModPhys.65.803). S2CID 119546199 (https://api.semanticscholar.org/CorpusID:119546199).
50. Shimony, Abner (1984). "Contextual Hidden Variable Theories and Bell's Inequalities". *British Journal for the Philosophy of Science*. **35** (1): 25–45. doi:10.1093/bjps/35.1.25 (https://doi.org/10.1093%2Fbjps%2F35.1.25).
51. Peres, Asher (1991). "Two simple proofs of the Kochen-Specker theorem" (http://stacks.iop.org/0305-4470/24/i=4/a=003). *Journal of Physics A: Mathematical and General*. **24** (4): L175–L178. Bibcode:1991JPhA...24L.175P (https://ui.adsabs.harvard.edu/abs/1991JPhA...24L.175P). doi:10.1088/0305-4470/24/4/003 (https://doi.org/10.1088%2F0305-4470%2F24%2F4%2F003). ISSN 0305-4470 (https://search.worldcat.org/issn/0305-4470).
52. Whitaker, Andrew (2016). *John Stewart Bell and Twentieth Century Physics: Vision and Integrity* (https://books.google.com/books?id=3Rg9DAAAQBAJ&q=fizika). Oxford University Press. ISBN 978-0-19-874299-9.
53. Bell, J. S. (1966). "On the problem of hidden variables in quantum mechanics". *Reviews of Modern Physics*. **38** (3): 447–452. Bibcode:1966RvMP...38..447B (https://ui.adsabs.harvard.edu/abs/1966RvMP...38..447B). doi:10.1103/revmodphys.38.447 (https://doi.org/10.1103%2Frevmodphys.38.447). OSTI 1444158 (https://www.osti.gov/biblio/1444158).
54. Kaiser, David (2012-01-30). "How the Hippies Saved Physics: Science, Counterculture, and the Quantum Revival [Excerpt]" (https://www.scientificamerican.com/article/how-the-hippies-saved-physics-science-counterculture-and-quantum-revival-excerpt/). *Scientific American*. Retrieved 2020-02-11.
55. Freedman, S. J.; Clauser, J. F. (1972). "Experimental test of local hidden-variable theories" (https://www.rpi.edu/dept/phys/Courses/PHYS4100/S06/BellsInequ1972.pdf) (PDF). *Physical Review Letters*. **28** (938): 938–941. Bibcode:1972PhRvL..28..938F (https://ui.adsabs.harvard.edu/abs/1972PhRvL..28..938F). doi:10.1103/PhysRevLett.28.938 (https://doi.org/10.1103%2FPhysRevLett.28.938).
56. Freedman, Stuart Jay (1972-05-05). *Experimental test of local hidden-variable theories* (https://escholarship.org/content/qt2f18n5nk/qt2f18n5nk.pdf?t=p2au19) (PDF) (PhD). University of California, Berkeley.
57. Aspect, Alain; Dalibard, Jean; Roger, Gérard (1982). "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers" (https://doi.org/10.1103%2FPhysRevLett.49.1804). *Physical Review Letters*. **49** (25): 1804–7. Bibcode:1982PhRvL..49.1804A (https://ui.adsabs.harvard.edu/abs/1982PhRvL..49.1804A). doi:10.1103/PhysRevLett.49.1804 (https://doi.org/10.1103%2FPhysRevLett.49.1804).
58. Pan, Jian-Wei; Bouwmeester, D.; Daniell, M.; Weinfurter, H.; Zeilinger, A. (2000). "Experimental test of quantum nonlocality in three-photon GHZ entanglement". *Nature*. **403** (6769): 515–519. Bibcode:2000Natur.403..515P (https://ui.adsabs.harvard.edu/abs/2000Natur.403..515P). doi:10.1038/35000514 (https://doi.org/10.1038%2F35000514). PMID 10676953 (https://pubmed.ncbi.nlm.nih.gov/10676953). S2CID 4309261 (https://api.semanticscholar.org/CorpusID:4309261).
59. Dehlinger, Dietrich; Mitchell, M. W. (2002). "Entangled photons, nonlocality, and Bell inequalities in the undergraduate laboratory". *American Journal of Physics*. **70** (9): 903–910. arXiv:quant-ph/0205171 (https://arxiv.org/abs/quant-ph/0205171). Bibcode:2002AmJPh..70..903D (https://ui.adsabs.harvard.edu/abs/2002AmJPh..70..903D). doi:10.1119/1.1498860 (https://doi.org/10.1119%2F1.1498860). S2CID 49487096 (https://api.semanticscholar.org/CorpusID:49487096).

60. Larsson, Jan-Åke (2014). "Loopholes in Bell inequality tests of local realism". *Journal of Physics A: Mathematical and Theoretical*. **47** (42): 424003. arXiv:1407.0363 (https://arxiv.org/abs/1407.0363). Bibcode:2014JPhA...47P4003L (https://ui.adsabs.harvard.edu/abs/2014JPhA...47P4003L). doi:10.1088/1751-8113/47/42/424003 (https://doi.org/10.1088%2F1751-8113%2F47%2F42%2F424003). S2CID 40332044 (https://api.semanticscholar.org/CorpusID:40332044).
61. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Scarani, V.; et al. (2011). "Experimentally faking the violation of Bell's inequalities". *Physical Review Letters*. **107** (17): 170404. arXiv:1106.3224 (https://arxiv.org/abs/1106.3224). Bibcode:2011PhRvL.107q0404G (https://ui.adsabs.harvard.edu/abs/2011PhRvL.107q0404G). doi:10.1103/PhysRevLett.107.170404 (https://doi.org/10.1103%2FPhysRevLett.107.170404). PMID 22107491 (https://pubmed.ncbi.nlm.nih.gov/22107491). S2CID 16306493 (https://api.semanticscholar.org/CorpusID:16306493).
62. Merali, Zeeya (27 August 2015). "Quantum 'spookiness' passes toughest test yet" (https://doi.org/10.1038%2Fnature.2015.18255). *Nature News*. **525** (7567): 14–15. Bibcode:2015Natur.525...14M (https://ui.adsabs.harvard.edu/abs/2015Natur.525...14M). doi:10.1038/nature.2015.18255 (https://doi.org/10.1038%2Fnature.2015.18255). PMID 26333448 (https://pubmed.ncbi.nlm.nih.gov/26333448). S2CID 4409566 (https://api.semanticscholar.org/CorpusID:4409566).
63. Markoff, Jack (21 October 2015). "Sorry, Einstein. Quantum Study Suggests 'Spooky Action' Is Real" (https://www.nytimes.com/2015/10/22/science/quantum-theory-experiment-said-to-prove-spooky-interactions.html). *New York Times*. Retrieved 21 October 2015.
64. Hensen, B.; et al. (21 October 2015). "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". *Nature*. **526** (7575): 682–686. arXiv:1508.05949 (https://arxiv.org/abs/1508.05949). Bibcode:2015Natur.526..682H (https://ui.adsabs.harvard.edu/abs/2015Natur.526..682H). doi:10.1038/nature15759 (https://doi.org/10.1038%2Fnature15759). PMID 26503041 (https://pubmed.ncbi.nlm.nih.gov/26503041). S2CID 205246446 (https://api.semanticscholar.org/CorpusID:205246446).
65. Shalm, L. K.; et al. (16 December 2015). "Strong Loophole-Free Test of Local Realism" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5815856). *Physical Review Letters*. **115** (25): 250402. arXiv:1511.03189 (https://arxiv.org/abs/1511.03189). Bibcode:2015PhRvL.115y0402S (https://ui.adsabs.harvard.edu/abs/2015PhRvL.115y0402S). doi:10.1103/PhysRevLett.115.250402 (https://doi.org/10.1103%2FPhysRevLett.115.250402). PMC 5815856 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5815856). PMID 26722906 (https://pubmed.ncbi.nlm.nih.gov/26722906).
66. Giustina, M.; et al. (16 December 2015). "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". *Physical Review Letters*. **115** (25): 250401. arXiv:1511.03190 (https://arxiv.org/abs/1511.03190). Bibcode:2015PhRvL.115y0401G (https://ui.adsabs.harvard.edu/abs/2015PhRvL.115y0401G). doi:10.1103/PhysRevLett.115.250401 (https://doi.org/10.1103%2FPhysRevLett.115.250401). PMID 26722905 (https://pubmed.ncbi.nlm.nih.gov/26722905). S2CID 13789503 (https://api.semanticscholar.org/CorpusID:13789503).
67. Aspect, Alain (December 16, 2015). "Closing the Door on Einstein and Bohr's Quantum Debate" (https://doi.org/10.1103%2FPhysics.8.123). *Physics*. **8**: 123. Bibcode:2015PhyOJ...8..123A (https://ui.adsabs.harvard.edu/abs/2015PhyOJ...8..123A). doi:10.1103/Physics.8.123 (https://doi.org/10.1103%2FPhysics.8.123).
68. Ahlander, Johan; Burger, Ludwig; Pollard, Niklas (2022-10-04). "Nobel physics prize goes to sleuths of 'spooky' quantum science" (https://www.reuters.com/world/aspect-clauser-zeilinger-win-2022-nobel-prize-physics-2022-10-04/). *Reuters*. Retrieved 2022-10-04.

69. Schlosshauer, Maximilian; Kofler, Johannes; Zeilinger, Anton (2013-01-06). "A Snapshot of Foundational Attitudes Toward Quantum Mechanics". *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*. **44** (3): 222–230. arXiv:1301.1069 (https://arxiv.org/abs/1301.1069). Bibcode:2013SHPMP..44..222S (https://ui.adsabs.harvard.edu/abs/2013SHPMP..44..222S). doi:10.1016/j.shpsb.2013.04.004 (https://doi.org/10.1016%2Fj.shpsb.2013.04.004). S2CID 55537196 (https://api.semanticscholar.org/CorpusID:55537196).
70. Werner, Reinhard F. (2014-10-24). "Comment on 'What Bell did' ". *Journal of Physics A: Mathematical and Theoretical*. **47** (42): 424011. Bibcode:2014JPhA...47P4011W (https://ui.adsabs.harvard.edu/abs/2014JPhA...47P4011W). doi:10.1088/1751-8113/47/42/424011 (https://doi.org/10.1088%2F1751-8113%2F47%2F42%2F424011). ISSN 1751-8113 (https://search.worldcat.org/issn/1751-8113). S2CID 122180759 (https://api.semanticscholar.org/CorpusID:122180759).
71. Żukowski, Marek (2017). "Bell's Theorem Tells Us Not What Quantum Mechanics is, but What Quantum Mechanics is Not". In Bertlmann, Reinhold; Zeilinger, Anton (eds.). *Quantum [Un]Speakables II*. The Frontiers Collection. Cham: Springer International Publishing. pp. 175–185. arXiv:1501.05640 (https://arxiv.org/abs/1501.05640). doi:10.1007/978-3-319-38987-5_10 (https://doi.org/10.1007%2F978-3-319-38987-5_10). ISBN 978-3-319-38985-1. S2CID 119214547 (https://api.semanticscholar.org/CorpusID:119214547).
72. Omnès, R. (1994). *The Interpretation of Quantum Mechanics*. Princeton University Press. ISBN 978-0-691-03669-4. OCLC 439453957 (https://search.worldcat.org/oclc/439453957).
73. Peierls, Rudolf (1979). *Surprises in Theoretical Physics*. Princeton University Press. pp. 26–29. ISBN 0-691-08241-3.
74. Mermin, N. D. (1999). "What Do These Correlations Know About Reality? Nonlocality and the Absurd". *Foundations of Physics*. **29** (4): 571–587. arXiv:quant-ph/9807055 (https://arxiv.org/abs/quant-ph/9807055). Bibcode:1998quant.ph..7055M (https://ui.adsabs.harvard.edu/abs/1998quant.ph..7055M). doi:10.1023/A:1018864225930 (https://doi.org/10.1023%2FA%3A1018864225930).
75. Hohenberg, P. C. (2010-10-05). "Colloquium : An introduction to consistent quantum theory". *Reviews of Modern Physics*. **82** (4): 2835–2844. arXiv:0909.2359 (https://arxiv.org/abs/0909.2359). Bibcode:2010RvMP...82.2835H (https://ui.adsabs.harvard.edu/abs/2010RvMP...82.2835H). doi:10.1103/RevModPhys.82.2835 (https://doi.org/10.1103%2FRevModPhys.82.2835). ISSN 0034-6861 (https://search.worldcat.org/issn/0034-6861). S2CID 20551033 (https://api.semanticscholar.org/CorpusID:20551033).
76. Healey, Richard (2016). "Quantum-Bayesian and Pragmatist Views of Quantum Theory" (https://plato.stanford.edu/entries/quantum-bayesian/). In Zalta, Edward N. (ed.). *Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University. Archived (https://web.archive.org/web/20210817204745/https://plato.stanford.edu/entries/quantum-bayesian/) from the original on 2021-08-17. Retrieved 2021-09-16.
77. Brown, Harvey R.; Timpson, Christopher G. (2016). "Bell on Bell's Theorem: The Changing Face of Nonlocality". In Bell, Mary; Gao, Shan (eds.). *Quantum Nonlocality and Reality: 50 years of Bell's theorem*. Cambridge University Press. pp. 91–123. arXiv:1501.03521 (https://arxiv.org/abs/1501.03521). doi:10.1017/CBO9781316219393.008 (https://doi.org/10.1017%2FCBO9781316219393.008). ISBN 9781316219393. S2CID 118686956 (https://api.semanticscholar.org/CorpusID:118686956).
78. Deutsch, David; Hayden, Patrick (2000). "Information flow in entangled quantum systems". *Proceedings of the Royal Society A*. **456** (1999): 1759–1774. arXiv:quant-ph/9906007 (https://arxiv.org/abs/quant-ph/9906007). Bibcode:2000RSPSA.456.1759D (https://ui.adsabs.harvard.edu/abs/2000RSPSA.456.1759D). doi:10.1098/rspa.2000.0585 (https://doi.org/10.1098%2Frspa.2000.0585). S2CID 13998168 (https://api.semanticscholar.org/CorpusID:13998168).

79. Jaynes, E. T. (1989). "Clearing up Mysteries — the Original Goal". *Maximum Entropy and Bayesian Methods* (http://bayes.wustl.edu/etj/articles/cmystery.pdf) (PDF). pp. 1–27. CiteSeerX 10.1.1.46.1264 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.1264). doi:10.1007/978-94-015-7860-8_1 (https://doi.org/10.1007%2F978-94-015-7860-8_1). ISBN 978-90-481-4044-2. Archived (https://web.archive.org/web/20111028131916/http://bayes.wustl.edu/etj/articles/cmystery.pdf) (PDF) from the original on 2011-10-28. Retrieved 2011-10-18.
80. Gill, Richard D. (2002). "Time, Finite Statistics, and Bell's Fifth Position". *Proceedings of the Conference Foundations of Probability and Physics - 2 : Växjö (Soland), Sweden, June 2-7, 2002*. Vol. 5. Växjö University Press. pp. 179–206. arXiv:quant-ph/0301059 (https://arxiv.org/abs/quant-ph/0301059).
81. Wood, Christopher J.; Spekkens, Robert W. (2015-03-03). "The lesson of causal discovery algorithms for quantum correlations: causal explanations of Bell-inequality violations require fine-tuning" (https://iopscience.iop.org/article/10.1088/1367-2630/17/3/033002). *New Journal of Physics*. **17** (3): 033002. arXiv:1208.4119 (https://arxiv.org/abs/1208.4119). Bibcode:2015NJPh...17c3002W (https://ui.adsabs.harvard.edu/abs/2015NJPh...17c3002W). doi:10.1088/1367-2630/17/3/033002 (https://doi.org/10.1088%2F1367-2630%2F17%2F3%2F033002). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 118518558 (https://api.semanticscholar.org/CorpusID:118518558).
82. Gröblacher, Simon; Paterek, Tomasz; Kaltenbaek, Rainer; Brukner, Časlav; Żukowski, Marek; Aspelmeyer, Markus; Zeilinger, Anton (2007). "An experimental test of non-local realism". *Nature*. **446** (7138): 871–5. arXiv:0704.2529 (https://arxiv.org/abs/0704.2529). Bibcode:2007Natur.446..871G (https://ui.adsabs.harvard.edu/abs/2007Natur.446..871G). doi:10.1038/nature05677 (https://doi.org/10.1038%2Fnature05677). PMID 17443179 (https://pubmed.ncbi.nlm.nih.gov/17443179). S2CID 4412358 (https://api.semanticscholar.org/CorpusID:4412358).
83. Kastner, Ruth E. (May 2010). "The quantum liar experiment in Cramer's transactional interpretation" (https://linkinghub.elsevier.com/retrieve/pii/S135521981000002X). *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*. **41** (2): 86–92. arXiv:0906.1626 (https://arxiv.org/abs/0906.1626). Bibcode:2010SHPMP..41...86K (https://ui.adsabs.harvard.edu/abs/2010SHPMP..41...86K). doi:10.1016/j.shpsb.2010.01.001 (https://doi.org/10.1016%2Fj.shpsb.2010.01.001). S2CID 16242184 (https://api.semanticscholar.org/CorpusID:16242184). Archived (https://web.archive.org/web/20180624053010/https://linkinghub.elsevier.com/retrieve/pii/S135521981000002X) from the original on 2018-06-24. Retrieved 2021-09-16.
84. 't Hooft, Gerard (2016). *The Cellular Automaton Interpretation of Quantum Mechanics* (http://www.oapen.org/search?identifier=1002003). Fundamental Theories of Physics. Vol. 185. Springer. doi:10.1007/978-3-319-41285-6 (https://doi.org/10.1007%2F978-3-319-41285-6). ISBN 978-3-319-41284-9. OCLC 951761277 (https://search.worldcat.org/oclc/951761277). S2CID 7779840 (https://api.semanticscholar.org/CorpusID:7779840). Archived (https://web.archive.org/web/20211229062338/https://library.oapen.org/handle/20.500.12657/27994) from the original on 2021-12-29. Retrieved 2020-08-27.

Further reading

The following are intended for general audiences.

- Aczel, Amir D. (2001). *Entanglement: The greatest mystery in physics*. New York: Four Walls Eight Windows.
- Afriat, A.; Selleri, F. (1999). *The Einstein, Podolsky and Rosen Paradox*. New York and London: Plenum Press.
- Baggott, J. (1992). *The Meaning of Quantum Theory*. Oxford University Press.

- Gilder, Louisa (2008). *The Age of Entanglement: When Quantum Physics Was Reborn*. New York: Alfred A. Knopf.
- Greene, Brian (2004). *The Fabric of the Cosmos*. Vintage. ISBN 0-375-72720-5.
- Mermin, N. David (1981). "Bringing home the atomic world: Quantum mysteries for anybody". *American Journal of Physics*. **49** (10): 940–943. Bibcode:1981AmJPh..49..940M (https://ui.adsabs.harvard.edu/abs/1981AmJPh..49..940M). doi:10.1119/1.12594 (https://doi.org/10.1119%2F1.12594). S2CID 122724592 (https://api.semanticscholar.org/CorpusID:122724592).
- Mermin, N. David (April 1985). "Is the moon there when nobody looks? Reality and the quantum theory". *Physics Today*. **38** (4): 38–47. Bibcode:1985PhT....38d..38M (https://ui.adsabs.harvard.edu/abs/1985PhT....38d..38M). doi:10.1063/1.880968 (https://doi.org/10.1063%2F1.880968).

The following are more technically oriented.

- Aspect, A.; et al. (1981). "Experimental Tests of Realistic Local Theories via Bell's Theorem" (https://doi.org/10.1103%2Fphysrevlett.47.460). *Phys. Rev. Lett*. **47** (7): 460–463. Bibcode:1981PhRvL..47..460A (https://ui.adsabs.harvard.edu/abs/1981PhRvL..47..460A). doi:10.1103/physrevlett.47.460 (https://doi.org/10.1103%2Fphysrevlett.47.460).
- Aspect, A.; et al. (1982). "Experimental Realization of Einstein–Podolsky–Rosen–Bohm Gedankenexperiment: A New Violation of Bell's Inequalities" (https://doi.org/10.1103%2Fphysrevlett.49.91). *Phys. Rev. Lett*. **49** (2): 91–94. Bibcode:1982PhRvL..49...91A (https://ui.adsabs.harvard.edu/abs/1982PhRvL..49...91A). doi:10.1103/physrevlett.49.91 (https://doi.org/10.1103%2Fphysrevlett.49.91).
- Aspect, A.; Grangier, P. (1985). "About resonant scattering and other hypothetical effects in the Orsay atomic-cascade experiment tests of Bell inequalities: a discussion and some new experimental data". *Lettere al Nuovo Cimento*. **43** (8): 345–348. doi:10.1007/bf02746964 (https://doi.org/10.1007%2Fbf02746964). S2CID 120840672 (https://api.semanticscholar.org/CorpusID:120840672).
- Bell, J. S. (1971). "Introduction to the hidden variable question". *Proceedings of the International School of Physics 'Enrico Fermi', Course IL, Foundations of Quantum Mechanics*. pp. 171–81.
- Bell, J. S. (2004). "Bertlmann's Socks and the Nature of Reality". *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press. pp. 139–158.
- D'Espagnat, B. (1979). "The Quantum Theory and Reality" (http://www.sciam.com/media/pdf/197911_0158.pdf) (PDF). *Scientific American*. **241** (5): 158–181. Bibcode:1979SciAm.241e.158D (https://ui.adsabs.harvard.edu/abs/1979SciAm.241e.158D). doi:10.1038/scientificamerican1179-158 (https://doi.org/10.1038%2Fscientificamerican1179-158). Archived (https://web.archive.org/web/20090327023619/http://www.sciam.com/media/pdf/197911_0158.pdf) (PDF) from the original on 2009-03-27. Retrieved 2009-03-18.
- Fry, E. S.; Walther, T.; Li, S. (1995). "Proposal for a loophole-free test of the Bell inequalities" (http://oaktrust.library.tamu.edu/bitstream/1969.1/126533/1/PhysRevA.52.4381.pdf) (PDF). *Phys. Rev. A*. **52** (6): 4381–4395. Bibcode:1995PhRvA..52.4381F (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.4381F). doi:10.1103/physreva.52.4381 (https://doi.org/10.1103%2Fphysreva.52.4381). hdl:1969.1/126533 (https://hdl.handle.net/1969.1%2F126533). PMID 9912775 (https://pubmed.ncbi.nlm.nih.gov/9912775). Archived (https://web.archive.org/web/20211229062332/http://oaktrust.library.tamu.edu/bitstream/handle/1969.1/126533/PhysRevA.52.4381.pdf;jsessionid=50AFAA1E4F54828C672C8FF01C56B167?sequence=1) from the original on 2021-12-29. Retrieved 2018-03-19.
- Fry, E. S.; Walther, T. (2002). "Atom based tests of the Bell Inequalities — the legacy of John Bell continues". In Bertlmann, R. A.; Zeilinger, A. (eds.). *Quantum [Un]speakables*. Berlin-Heidelberg-New York: Springer. pp. 103–117.

- Goldstein, Sheldon; et al. (2011). "Bell's theorem" (https://doi.org/10.4249%2Fscholarpedia.8378). *Scholarpedia*. **6** (10): 8378. Bibcode:2011SchpJ...6.8378G (https://ui.adsabs.harvard.edu/abs/2011SchpJ...6.8378G). doi:10.4249/scholarpedia.8378 (https://doi.org/10.4249%2Fscholarpedia.8378).
- Griffiths, R. B. (2001). *Consistent Quantum Theory*. Cambridge University Press. ISBN 978-0-521-80349-6. OCLC 1180958776 (https://search.worldcat.org/oclc/1180958776).
- Hardy, L. (1993). "Nonlocality for 2 particles without inequalities for almost all entangled states". *Physical Review Letters*. **71** (11): 1665–1668. Bibcode:1993PhRvL..71.1665H (https://ui.adsabs.harvard.edu/abs/1993PhRvL..71.1665H). doi:10.1103/physrevlett.71.1665 (https://doi.org/10.1103%2Fphysrevlett.71.1665). PMID 10054467 (https://pubmed.ncbi.nlm.nih.gov/10054467). S2CID 11839894 (https://api.semanticscholar.org/CorpusID:11839894).
- Matsukevich, D. N.; Maunz, P.; Moehring, D. L.; Olmschenk, S.; Monroe, C. (2008). "Bell Inequality Violation with Two Remote Atomic Qubits". *Phys. Rev. Lett*. **100** (15): 150404. arXiv:0801.2184 (https://arxiv.org/abs/0801.2184). Bibcode:2008PhRvL.100o0404M (https://ui.adsabs.harvard.edu/abs/2008PhRvL.100o0404M). doi:10.1103/physrevlett.100.150404 (https://doi.org/10.1103%2Fphysrevlett.100.150404). PMID 18518088 (https://pubmed.ncbi.nlm.nih.gov/18518088). S2CID 11536757 (https://api.semanticscholar.org/CorpusID:11536757).
- Rieffel, Eleanor G.; Polak, Wolfgang H. (4 March 2011). "4.4 EPR Paradox and Bell's Theorem". *Quantum Computing: A Gentle Introduction*. MIT Press. pp. 60–65. ISBN 978-0-262-01506-6.
- Sulcs, S. (2003). "The Nature of Light and Twentieth Century Experimental Physics". *Foundations of Science*. **8** (4): 365–391. doi:10.1023/A:1026323203487 (https://doi.org/10.1023%2FA%3A1026323203487). S2CID 118769677 (https://api.semanticscholar.org/CorpusID:118769677).
- van Fraassen, B. C. (1991). *Quantum Mechanics: An Empiricist View*. Clarendon Press. ISBN 978-0-198-24861-3. OCLC 22906474 (https://search.worldcat.org/oclc/22906474).

External links

- Mermin: Spooky Actions At A Distance? Oppenheimer Lecture (https://www.youtube.com/watch?v=ta09WXiUqcQ).
- "Bell's theorem" (http://www.iep.utm.edu/epr). *Internet Encyclopedia of Philosophy*.
- "Bell inequalities" (https://www.encyclopediaofmath.org/index.php?title=Bell_inequalities). *Encyclopedia of Mathematics*. EMS Press. 2001 [1994].

Retrieved from "https://en.wikipedia.org/w/index.php?title=Bell%27s_theorem&oldid=1245568239"

WIKIPEDIA
The Free Encyclopedia

Eastin–Knill theorem

The **Eastin–Knill theorem** is a no-go theorem that states: "No quantum error correcting code can have a continuous symmetry which acts transversely on physical qubits".[1] In other words, no quantum error correcting code can transversely implement a universal gate set, where a transversal logical gate is one that can be implemented on a logical qubit by the independent action of separate physical gates on corresponding physical qubits.

In addition to investigating fault tolerant quantum computation, the Eastin–Knill theorem is also useful for studying quantum gravity via the AdS/CFT correspondence and in condensed matter physics via quantum reference frame[2] or many-body theory.[3]

The theorem is named after Bryan Eastin and Emanuel Knill, who published it in 2009.[1]

Description

Since quantum computers are inherently noisy, quantum error correcting codes are used to correct errors that affect information due to decoherence and dissipation. Decoding error corrected data in order to perform gates on the qubits makes it prone to errors. Fault tolerant quantum computation avoids this by performing gates on encoded data. Transversal gates, which perform a gate between two logical qubits each of which is encoded in N physical qubits by pairing up the physical qubits of each encoded qubit ("code block"), and performing independent gates on each pair, can be used to perform fault tolerant but not universal quantum computation because they guarantee that errors don't spread uncontrollably through the computation. This is because transversal gates ensure that each qubit in a code block is acted on by at most a single physical gate and each code block is corrected independently when an error occurs.

The Eastin–Knill theorem implies that a universal set like $\{H, S, \mathrm{CNOT}, T\}$ gates can't be implemented transversally. For example, the T gate can't be implemented transversely in the Steane code.[4] This calls for ways of circumventing Eastin–Knill in order to perform fault tolerant quantum computation.

Approximate Eastin–Knill theorem

The approximate version of the Eastin–Knill theorem states: "If a code admits a continuous symmetry pertaining to a Lie group and corrects erasure with fixed accuracy, then for each logical qubit, a number of physical qubits per subsystem that is inversely proportional to the error parameter is needed".[2][3][5] The approximate version of the Eastin–Knill theorem is more robust than the original because it explains

why it's impossible to have continuous symmetries for transversal gates on the microscopic scale while also explaining how it's possible to have continuous symmetries for transversal gates on the macroscopic scale.

Circumventing the theorem

The Eastin–Knill theorem does not prohibit protocols that provide fault tolerant quantum computation. Some methods of getting around Eastin–Knill are:

- Code switching[6]
- Code drift[7]
- Using continuous variables[2][3][5]
- Shor's fault tolerant toffoli gate[8]
- Teleportation of gates[9]
- Magic state distillation[10]
- Multiple partitions [11]
- Pieceable fault tolerance [12]
- Universal braiding[13]

References

1. Eastin, Bryan; Knill, Emanuel (2009). "Restrictions on Transversal Encoded Quantum Gate Sets". *Physical Review Letters*. **102** (11): 110502. arXiv:0811.4262 (https://arxiv.org/abs/0811.4262). Bibcode:2009PhRvL.102k0502E (https://ui.adsabs.harvard.edu/abs/2009PhRvL.102k0502E). doi:10.1103/PhysRevLett.102.110502 (https://doi.org/10.1103%2FPhysRevLett.102.110502). PMID 19392181 (https://pubmed.ncbi.nlm.nih.gov/19392181). S2CID 44457708 (https://api.semanticscholar.org/CorpusID:44457708).
2. Woods, Mischa; Alhambra, Alvaro M. (2020). "Continuous groups of transversal gates for quantum error correcting codes from finite clock reference frames". *Quantum*. **4**: 245. arXiv:1902.07725 (https://arxiv.org/abs/1902.07725). Bibcode:2020Quant...4..245W (https://ui.adsabs.harvard.edu/abs/2020Quant...4..245W). doi:10.22331/q-2020-03-23-245 (https://doi.org/10.22331%2Fq-2020-03-23-245). S2CID 119302752 (https://api.semanticscholar.org/CorpusID:119302752).
3. Faist, Philippe; Nezami, Sepehr; V. Albert, Victor; Salton, Grant; Pastawski, Fernando; Hayden, Patrick; Preskill, John (2020). "Continuous Symmetries and Approximate Quantum Error Correction". *Physical Review X*. **10** (4): 041018. arXiv:1902.07714 (https://arxiv.org/abs/1902.07714). Bibcode:2020PhRvX..10d1018F (https://ui.adsabs.harvard.edu/abs/2020PhRvX..10d1018F). doi:10.1103/PhysRevX.10.041018 (https://doi.org/10.1103%2FPhysRevX.10.041018). S2CID 119207861 (https://api.semanticscholar.org/CorpusID:119207861).
4. Campbell, Earl T.; Terhal, Barbara M.; Vuillot, Christophe (2016). "Roads towards fault-tolerant universal quantum computation". *Nature*. **549** (7671): 172–179. arXiv:quant-ph/0403025 (https://arxiv.org/abs/quant-ph/0403025). Bibcode:2017Natur.549..172C (https://ui.adsabs.harvard.edu/abs/2017Natur.549..172C). doi:10.1038/nature23460 (https://doi.org/10.1038%2Fnature23460). PMID 28905902 (https://pubmed.ncbi.nlm.nih.gov/28905902). S2CID 4446310 (https://api.semanticscholar.org/CorpusID:4446310).

5. Yang, Yuxiang; Mo, Yin; Renes, Joseph M.; Chiribella, Giulio; Woods, Mischa (2022). "Optimal universal quantum error correction via bounded reference frames". *Physical Review Research*. **4** (2): 023107. arXiv:2007.09154 (https://arxiv.org/abs/2007.09154). Bibcode:2022PhRvR...4b3107Y (https://ui.adsabs.harvard.edu/abs/2022PhRvR...4b3107Y). doi:10.1103/PhysRevResearch.4.023107 (https://doi.org/10.1103%2FPhysRevResearch.4.023107). S2CID 244488748 (https://api.semanticscholar.org/CorpusID:244488748).
6. Duclos-Cianci, Guillaume; Poulin, David (2014). "Reducing the quantum computing overhead with complex gate distillation". *Physical Review A*. **91** (4): 042315. arXiv:1309.3310 (https://arxiv.org/abs/1309.3310). doi:10.1103/PhysRevA.91.042315 (https://doi.org/10.1103%2FPhysRevA.91.042315). S2CID 73589915 (https://api.semanticscholar.org/CorpusID:73589915).
7. Paetznick, Adam; Reichardt, Ben W. (2014). "Universal fault-tolerant quantum computation with only transversal gates and error correction". *Physical Review Letters*. **111** (9): 090505. arXiv:1309.3310 (https://arxiv.org/abs/1309.3310). doi:10.1103/PhysRevLett.111.090505 (https://doi.org/10.1103%2FPhysRevLett.111.090505). PMID 24033013 (https://pubmed.ncbi.nlm.nih.gov/24033013). S2CID 20659050 (https://api.semanticscholar.org/CorpusID:20659050).
8. Shor, Peter (1996). "Fault-tolerant quantum computation". *Proceedings of 37th Conference on Foundations of Computer Science*. Vol. 102. pp. 56–65. doi:10.1109/SFCS.1996.548464 (https://doi.org/10.1109%2FSFCS.1996.548464). ISBN 978-0-8186-7594-2. S2CID 7508572 (https://api.semanticscholar.org/CorpusID:7508572).
9. Gottesman, Daniel; Chuang, Isaac L. (1999). "Quantum Teleportation is a Universal Computational Primitive". *Nature*. **402** (6760): 390–393. arXiv:quant-ph/9908010 (https://arxiv.org/abs/quant-ph/9908010). Bibcode:1999Natur.402..390G (https://ui.adsabs.harvard.edu/abs/1999Natur.402..390G). doi:10.1038/46503 (https://doi.org/10.1038%2F46503). S2CID 4411647 (https://api.semanticscholar.org/CorpusID:4411647).
10. Bravyi, Sergey; Kitaev, Alexei (2005). "Universal quantum computation with ideal Clifford gates and noisy ancillas". *Physical Review A*. **71** (2): 022316. arXiv:quant-ph/0403025 (https://arxiv.org/abs/quant-ph/0403025). Bibcode:2005PhRvA..71b2316B (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71b2316B). doi:10.1103/PhysRevA.71.022316 (https://doi.org/10.1103%2FPhysRevA.71.022316). S2CID 17504370 (https://api.semanticscholar.org/CorpusID:17504370).
11. Jochym-O'Connor, Tomas; Laflamme, Raymond (2013). "Using Concatenated Quantum Codes for Universal Fault-Tolerant Quantum Gates". *Physical Review Letters*. **112** (1): 010505. arXiv:quant-ph/0403025 (https://arxiv.org/abs/quant-ph/0403025). doi:10.1103/PhysRevLett.112.010505 (https://doi.org/10.1103%2FPhysRevLett.112.010505). PMID 24483879 (https://pubmed.ncbi.nlm.nih.gov/24483879). S2CID 23069274 (https://api.semanticscholar.org/CorpusID:23069274).
12. Yoder, Theodore J.; Takagi, Ryuji (2016). "Universal fault-tolerant gates on concatenated stabilizer codes". *Physical Review X*. **6** (3): 090505. arXiv:1603.03948 (https://arxiv.org/abs/1603.03948). Bibcode:2016PhRvX...6c1039Y (https://ui.adsabs.harvard.edu/abs/2016PhRvX...6c1039Y). doi:10.1103/PhysRevX.6.031039 (https://doi.org/10.1103%2FPhysRevX.6.031039). S2CID 39022969 (https://api.semanticscholar.org/CorpusID:39022969).
13. Levin, Michael A.; Wen, Xiao-Gang (2004). "String-net condensation: A physical mechanism for topological phases". *Physical Review B*. **71** (4): 045110. arXiv:cond-mat/0404617 (https://arxiv.org/abs/cond-mat/0404617). doi:10.1103/PhysRevB.71.045110 (https://doi.org/10.1103%2FPhysRevB.71.045110). S2CID 51962817 (https://api.semanticscholar.org/CorpusID:51962817).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Eastin–Knill_theorem&oldid=1221403903"

WIKIPEDIA
The Free Encyclopedia

Gleason's theorem

In mathematical physics, **Gleason's theorem** shows that the rule one uses to calculate probabilities in quantum physics, the Born rule, can be derived from the usual mathematical representation of measurements in quantum physics together with the assumption of non-contextuality. Andrew M. Gleason first proved the theorem in 1957,[1] answering a question posed by George W. Mackey, an accomplishment that was historically significant for the role it played in showing that wide classes of hidden-variable theories are inconsistent with quantum physics. Multiple variations have been proven in the years since. Gleason's theorem is of particular importance for the field of quantum logic and its attempt to find a minimal set of mathematical axioms for quantum theory.

Statement of the theorem

Conceptual background

In quantum mechanics, each physical system is associated with a Hilbert space. For the purposes of this overview, the Hilbert space is assumed to be finite-dimensional. In the approach codified by John von Neumann, a measurement upon a physical system is represented by a self-adjoint operator on that Hilbert space sometimes termed an "observable". The eigenvectors of such an operator form an orthonormal basis for the Hilbert space, and each possible outcome of that measurement corresponds to one of the vectors comprising the basis. A density operator is a positive-semidefinite operator on the Hilbert space whose trace is equal to 1. In the language of von Weizsäcker, a density operator is a "catalogue of probabilities": for each measurement that can be defined, the probability distribution over the outcomes of that measurement can be computed from the density operator.[2] The procedure for doing so is the Born rule, which states that

$$P(x_i) = \mathrm{Tr}(\Pi_i \rho),$$

where ρ is the density operator, and Π_i is the projection operator onto the basis vector corresponding to the measurement outcome x_i.

The Born rule associates a probability with each unit vector in the Hilbert space, in such a way that these probabilities sum to 1 for any set of unit vectors comprising an orthonormal basis. Moreover, the probability associated with a unit vector is a function of the density operator and the unit vector, and not of additional information like a choice of basis for that vector to be embedded in. Gleason's theorem establishes the converse: all assignments of probabilities to unit vectors (or, equivalently, to the operators that project onto them) that satisfy these conditions take the form of applying the Born rule to some density operator. Gleason's theorem holds if the dimension of the Hilbert space is 3 or greater; counterexamples exist for dimension 2.

Deriving the state space and the Born rule

The probability of any outcome of a measurement upon a quantum system must be a real number between 0 and 1 inclusive, and in order to be consistent, for any individual measurement the probabilities of the different possible outcomes must add up to 1. Gleason's theorem shows that any function that assigns probabilities to measurement outcomes, as identified by projection operators, must be expressible in terms of a density operator and the Born rule. This gives not only the rule for calculating probabilities, but also determines the set of possible quantum states.

Let f be a function from projection operators to the unit interval with the property that, if a set $\{\Pi_i\}$ of projection operators sum to the identity matrix (that is, if they correspond to an orthonormal basis), then

$$\sum_i f(\Pi_i) = 1.$$

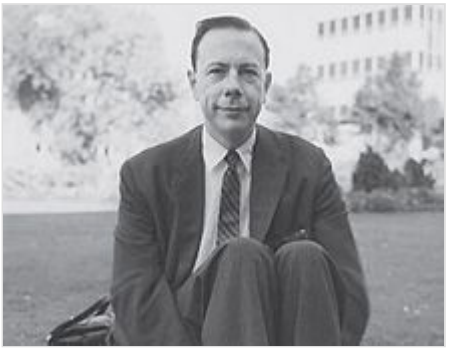
Such a function expresses an assignment of probability values to the outcomes of measurements, an assignment that is "noncontextual" in the sense that the probability for an outcome does not depend upon which measurement that outcome is embedded within, but only upon the mathematical representation of that specific outcome, i.e., its projection operator.[3][4]:§1.3[5]:§2.1[6] Gleason's theorem states that for any such function f, there exists a positive-semidefinite operator ρ with unit trace such that

$$f(\Pi_i) = \mathrm{Tr}(\Pi_i \rho).$$

Both the Born rule and the fact that "catalogues of probability" are positive-semidefinite operators of unit trace follow from the assumptions that measurements are represented by orthonormal bases, and that probability assignments are "noncontextual". In order for Gleason's theorem to be applicable, the space on which measurements are defined must be a real or complex Hilbert space, or a quaternionic module.[a] (Gleason's argument is inapplicable if, for example, one tries to construct an analogue of quantum mechanics using *p*-adic numbers.)

History and outline of Gleason's proof

In 1932, John von Neumann also managed to derive the Born rule in his textbook *Mathematische Grundlagen der Quantenmechanik* [*Mathematical Foundations of Quantum Mechanics*]. However, the assumptions on which von Neumann built his proof were rather strong and eventually regarded to not be well-motivated.[14] Specifically, von Neumann assumed that the probability function must be linear on all observables, commuting or non-commuting. His proof was derided by John Bell as "not merely false but foolish!".[15][16] Gleason, on the other hand, did not assume linearity, but merely additivity for commuting projectors together with noncontextuality, assumptions seen as better motivated and more physically meaningful.[16][17]


Gleason in 1959

By the late 1940s, George Mackey had grown interested in the mathematical foundations of quantum physics, wondering in particular whether the Born rule was the only possible rule for calculating probabilities in a theory that represented measurements as orthonormal bases on a Hilbert space.[18][19] Mackey discussed this problem with Irving Segal at the University of Chicago, who in turn raised it with

Richard Kadison, then a graduate student. Kadison showed that for 2-dimensional Hilbert spaces there exists a probability measure that does not correspond to quantum states and the Born rule. Gleason's result implies that this only happens in dimension 2.[19]

Gleason's original proof proceeds in three stages.[20]:§2 In Gleason's terminology, a *frame function* is a real-valued function f on the unit sphere of a Hilbert space such that

$$\sum_i f(x_i) = 1$$

whenever the vectors x_i comprise an orthonormal basis. A noncontextual probability assignment as defined in the previous section is equivalent to a frame function.[b] Any such measure that can be written in the standard way, that is, by applying the Born rule to a quantum state, is termed a *regular* frame function. Gleason derives a sequence of lemmas concerning when a frame function is necessarily regular, culminating in the final theorem. First, he establishes that every continuous frame function on the Hilbert space $\mathbb{R}^3$ is regular. This step makes use of the theory of spherical harmonics. Then, he proves that frame functions on $\mathbb{R}^3$ have to be continuous, which establishes the theorem for the special case of $\mathbb{R}^3$. This step is regarded as the most difficult of the proof.[21][22] Finally, he shows that the general problem can be reduced to this special case. Gleason credits one lemma used in this last stage of the proof to his doctoral student Richard Palais.[1]:fn 3

Robin Lyth Hudson described Gleason's theorem as "celebrated and notoriously difficult".[23] Cooke, Keane and Moran later produced a proof that is longer than Gleason's but requires fewer prerequisites.[21]

Implications

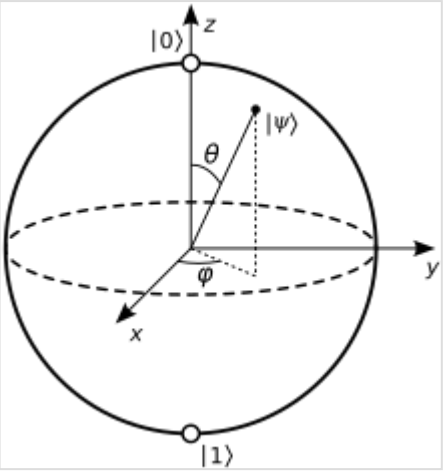
Gleason's theorem highlights a number of fundamental issues in quantum measurement theory. As Fuchs argues, the theorem "is an extremely powerful result", because "it indicates the extent to which the Born probability rule and even the state-space structure of density operators are *dependent* upon the theory's other postulates". In consequence, quantum theory is "a tighter package than one might have first thought".[24]:94–95 Various approaches to rederiving the quantum formalism from alternative axioms have, accordingly, employed Gleason's theorem as a key step, bridging the gap between the structure of Hilbert space and the Born rule.[c]

Hidden variables

Moreover, the theorem is historically significant for the role it played in ruling out the possibility of certain classes of hidden variables in quantum mechanics. A hidden-variable theory that is deterministic implies that the probability of a given outcome is *always* either 0 or 1. For example, a Stern–Gerlach measurement on a spin-1 atom will report that the atom's angular momentum along the chosen axis is one of three possible values, which can be designated $-$, 0 and $+$. In a deterministic hidden-variable theory, there exists an underlying physical property that fixes the result found in the measurement. Conditional on the value of the underlying physical property, any given outcome (for example, a result of $+$) must be either impossible or guaranteed. But Gleason's theorem implies that there can be no such deterministic probability measure. The mapping $u \to \langle \rho u, u \rangle$ is continuous on the unit sphere of the Hilbert space for any density operator ρ. Since this unit sphere is connected, no continuous probability measure on it can be deterministic.[26]:§1.3 Gleason's theorem therefore suggests that quantum theory represents a deep and

fundamental departure from the classical intuition that uncertainty is due to ignorance about hidden degrees of freedom.[27] More specifically, Gleason's theorem rules out hidden-variable models that are "noncontextual". Any hidden-variable model for quantum mechanics must, in order to avoid the implications of Gleason's theorem, involve hidden variables that are not properties belonging to the measured system alone but also dependent upon the external context in which the measurement is made. This type of dependence is often seen as contrived or undesirable; in some settings, it is inconsistent with special relativity.[27][28]

To construct a counterexample for 2-dimensional Hilbert space, known as a qubit, let the hidden variable be a unit vector $\vec{\lambda}$ in 3-dimensional Euclidean space. Using the Bloch sphere, each possible measurement on a qubit can be represented as a pair of antipodal points on the unit sphere. Defining the probability of a measurement outcome to be 1 if the point representing that outcome lies in the same hemisphere as $\vec{\lambda}$ and 0 otherwise yields an assignment of probabilities to measurement outcomes that obeys Gleason's assumptions. However, this probability assignment does not correspond to any valid density operator. By introducing a probability distribution over the possible values of $\vec{\lambda}$, a hidden-variable model for a qubit that reproduces the predictions of quantum theory can be constructed.[27][29]



In the Bloch sphere representation of a qubit, each point on the unit sphere stands for a pure state. All other density matrices correspond to points in the interior.

Gleason's theorem motivated later work by John Bell, Ernst Specker and Simon Kochen that led to the result often called the Kochen–Specker theorem, which likewise shows that noncontextual hidden-variable models are incompatible with quantum mechanics. As noted above, Gleason's theorem shows that there is no probability measure over the rays of a Hilbert space that only takes the values 0 and 1 (as long as the dimension of that space exceeds 2). The Kochen–Specker theorem refines this statement by constructing a specific finite subset of rays on which no such probability measure can be defined.[27][30] The fact that such a finite subset of rays must exist follows from Gleason's theorem by way of a logical compactness argument, but this method does not construct the desired set explicitly.[20]:§1 In the related no-hidden-variables result known as Bell's theorem, the assumption that the hidden-variable theory is noncontextual instead is replaced by the assumption that it is local. The same sets of rays used in Kochen–Specker constructions can also be employed to derive Bell-type proofs.[27][31][32]

Pitowsky uses Gleason's theorem to argue that quantum mechanics represents a new theory of probability, one in which the structure of the space of possible events is modified from the classical, Boolean algebra thereof. He regards this as analogous to the way that special relativity modifies the kinematics of Newtonian mechanics.[4][5]

The Gleason and Kochen–Specker theorems have been cited in support of various philosophies, including perspectivism, constructive empiricism and agential realism.[33][34][35]

Quantum logic

Gleason's theorem finds application in quantum logic, which makes heavy use of lattice theory. Quantum logic treats the outcome of a quantum measurement as a logical proposition and studies the relationships and structures formed by these logical propositions. They are organized into a lattice, in which the distributive law, valid in classical logic, is weakened, to reflect the fact that in quantum physics, not all pairs of quantities can be measured simultaneously.[36] The *representation theorem* in quantum logic shows that such a lattice is isomorphic to the lattice of subspaces of a vector space with a scalar product.[5]:§2 Using Solèr's theorem, the (skew) field K over which the vector space is defined can be proven, with additional hypotheses, to be either the real numbers, complex numbers, or the quaternions, as is needed for Gleason's theorem to hold.[12]:§3[37][38]

By invoking Gleason's theorem, the form of a probability function on lattice elements can be restricted. Assuming that the mapping from lattice elements to probabilities is noncontextual, Gleason's theorem establishes that it must be expressible with the Born rule.

Generalizations

Gleason originally proved the theorem assuming that the measurements applied to the system are of the von Neumann type, i.e., that each possible measurement corresponds to an orthonormal basis of the Hilbert space. Later, Busch[39] and independently Caves *et al.*[24]:116[40] proved an analogous result for a more general class of measurements, known as positive-operator-valued measures (POVMs). The set of all POVMs includes the set of von Neumann measurements, and so the assumptions of this theorem are significantly stronger than Gleason's. This made the proof of this result simpler than Gleason's, and the conclusions stronger. Unlike the original theorem of Gleason, the generalized version using POVMs also applies to the case of a single qubit.[41][42] Assuming noncontextuality for POVMs is, however, controversial, as POVMs are not fundamental, and some authors defend that noncontextuality should be assumed only for the underlying von Neumann measurements.[43] Gleason's theorem, in its original version, does not hold if the Hilbert space is defined over the rational numbers, i.e., if the components of vectors in the Hilbert space are restricted to be rational numbers, or complex numbers with rational parts. However, when the set of allowed measurements is the set of all POVMs, the theorem holds.[40]:§3.D

The original proof by Gleason was not constructive: one of the ideas on which it depends is the fact that every continuous function defined on a compact space attains its minimum. Because one cannot in all cases explicitly show where the minimum occurs, a proof that relies upon this principle will not be a constructive proof. However, the theorem can be reformulated in such a way that a constructive proof can be found.[20][44]

Gleason's theorem can be extended to some cases where the observables of the theory form a von Neumann algebra. Specifically, an analogue of Gleason's result can be shown to hold if the algebra of observables has no direct summand that is representable as the algebra of 2×2 matrices over a

commutative von Neumann algebra (i.e., no direct summand of type I_2). In essence, the only barrier to proving the theorem is the fact that Gleason's original result does not hold when the Hilbert space is that of a qubit.[45]

Notes

a. For additional discussion on this point, see Piron,[7]:§6 Drisch,[8] Horwitz and Biedenharn,[9] Razon and Horwitz,[10] Varadarajan,[11]:83 Cassinelli and Lahti,[12]:§2 and Moretti and Oppio.[13]

b. Gleason allows for the possibility that a frame function is normalized to a constant other than 1, but focusing on the case of "unit weight" as done here does not result in any loss of generality.

c. This is discussed by Barnum et al.,[3] Cassinelli and Lahti,[12]:§2 Stairs,[25] and Wilce.[26]:§1.4

References

1. Gleason, Andrew M. (1957). "Measures on the closed subspaces of a Hilbert space" (http://www.iumj.indiana.edu/IUMJ/FULLTEXT/1957/6/56050). *Indiana University Mathematics Journal*. **6** (4): 885–893. doi:10.1512/iumj.1957.6.56050 (https://doi.org/10.1512%2Fiumj.1957.6.56050). MR 0096113 (https://mathscinet.ams.org/mathscinet-getitem?mr=0096113).
2. Drieschner, M.; Görnitz, Th.; von Weizsäcker, C. F. (1988-03-01). "Reconstruction of abstract quantum theory". *International Journal of Theoretical Physics*. **27** (3): 289–306. Bibcode:1988IJTP...27..289D (https://ui.adsabs.harvard.edu/abs/1988IJTP...27..289D). doi:10.1007/bf00668895 (https://doi.org/10.1007%2Fbf00668895). ISSN 0020-7748 (https://search.worldcat.org/issn/0020-7748). S2CID 122866239 (https://api.semanticscholar.org/CorpusID:122866239).
3. Barnum, H.; Caves, C. M.; Finkelstein, J.; Fuchs, C. A.; Schack, R. (2000-05-08). "Quantum probability from decision theory?" (http://rspa.royalsocietypublishing.org/content/456/1997/1175). *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. **456** (1997): 1175–1182. arXiv:quant-ph/9907024 (https://arxiv.org/abs/quant-ph/9907024). Bibcode:2000RSPSA.456.1175B (https://ui.adsabs.harvard.edu/abs/2000RSPSA.456.1175B). CiteSeerX 10.1.1.769.8732 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.769.8732). doi:10.1098/rspa.2000.0557 (https://doi.org/10.1098%2Frspa.2000.0557). ISSN 1364-5021 (https://search.worldcat.org/issn/1364-5021). S2CID 11563591 (https://api.semanticscholar.org/CorpusID:11563591).
4. Pitowsky, Itamar (2003). "Betting on the outcomes of measurements: a Bayesian theory of quantum probability". *Studies in History and Philosophy of Modern Physics*. **34** (3): 395–414. arXiv:quant-ph/0208121 (https://arxiv.org/abs/quant-ph/0208121). Bibcode:2003SHPMP..34..395P (https://ui.adsabs.harvard.edu/abs/2003SHPMP..34..395P). doi:10.1016/S1355-2198(03)00035-2 (https://doi.org/10.1016%2FS1355-2198%2803%2900035-2).
5. Pitowsky, Itamar (2006). "Quantum mechanics as a theory of probability". In Demopoulos, William; Pitowsky, Itamar (eds.). *Physical Theory and its Interpretation: Essays in Honor of Jeffrey Bub*. Springer. p. 213. arXiv:quant-ph/0510095 (https://arxiv.org/abs/quant-ph/0510095). Bibcode:2005quant.ph.10095P (https://ui.adsabs.harvard.edu/abs/2005quant.ph.10095P). ISBN 9781402048760. OCLC 917845122 (https://search.worldcat.org/oclc/917845122).

6. Kunjwal, Ravi; Spekkens, Rob W. (2015-09-09). "From the Kochen–Specker theorem to noncontextuality inequalities without assuming determinism". *Physical Review Letters*. **115** (11): 110403. arXiv:1506.04150 (https://arxiv.org/abs/1506.04150). Bibcode:2015PhRvL.115k0403K (https://ui.adsabs.harvard.edu/abs/2015PhRvL.115k0403K). doi:10.1103/PhysRevLett.115.110403 (https://doi.org/10.1103%2FPhysRevLett.115.110403). PMID 26406812 (https://pubmed.ncbi.nlm.nih.gov/26406812). S2CID 10308680 (https://api.semanticscholar.org/CorpusID:10308680).
7. Piron, C. (1972-10-01). "Survey of general quantum physics". *Foundations of Physics*. **2** (4): 287–314. Bibcode:1972FoPh....2..287P (https://ui.adsabs.harvard.edu/abs/1972FoPh....2..287P). doi:10.1007/bf00708413 (https://doi.org/10.1007%2Fbf00708413). ISSN 0015-9018 (https://search.worldcat.org/issn/0015-9018). S2CID 123364715 (https://api.semanticscholar.org/CorpusID:123364715).
8. Drisch, Thomas (1979-04-01). "Generalization of Gleason's theorem". *International Journal of Theoretical Physics*. **18** (4): 239–243. Bibcode:1979IJTP...18..239D (https://ui.adsabs.harvard.edu/abs/1979IJTP...18..239D). doi:10.1007/bf00671760 (https://doi.org/10.1007%2Fbf00671760). ISSN 0020-7748 (https://search.worldcat.org/issn/0020-7748). S2CID 121825926 (https://api.semanticscholar.org/CorpusID:121825926).
9. Horwitz, L. P.; Biedenharn, L. C. (1984). "Quaternion quantum mechanics: Second quantization and gauge fields". *Annals of Physics*. **157** (2): 432–488. Bibcode:1984AnPhy.157..432H (https://ui.adsabs.harvard.edu/abs/1984AnPhy.157..432H). doi:10.1016/0003-4916(84)90068-x (https://doi.org/10.1016%2F0003-4916%2884%2990068-x).
10. Razon, Aharon; Horwitz, L. P. (1991-08-01). "Projection operators and states in the tensor product of quaternion Hilbert modules". *Acta Applicandae Mathematicae*. **24** (2): 179–194. doi:10.1007/bf00046891 (https://doi.org/10.1007%2Fbf00046891). ISSN 0167-8019 (https://search.worldcat.org/issn/0167-8019). S2CID 119666741 (https://api.semanticscholar.org/CorpusID:119666741).
11. Varadarajan, Veeravalli S. (2007). *Geometry of Quantum Theory* (2nd ed.). Springer Science+Business Media. ISBN 978-0-387-96124-8. OCLC 764647569 (https://search.worldcat.org/oclc/764647569).
12. Cassinelli, G.; Lahti, P. (2017-11-13). "Quantum mechanics: why complex Hilbert space?" (https://doi.org/10.1098%2Frsta.2016.0393). *Philosophical Transactions of the Royal Society A*. **375** (2106): 20160393. Bibcode:2017RSPTA.37560393C (https://ui.adsabs.harvard.edu/abs/2017RSPTA.37560393C). doi:10.1098/rsta.2016.0393 (https://doi.org/10.1098%2Frsta.2016.0393). ISSN 1364-503X (https://search.worldcat.org/issn/1364-503X). PMID 28971945 (https://pubmed.ncbi.nlm.nih.gov/28971945).
13. Moretti, Valter; Oppio, Marco (2018-10-16). "The Correct Formulation of Gleason's Theorem in Quaternionic Hilbert Spaces". *Annales Henri Poincaré*. **19** (11): 3321–3355. arXiv:1803.06882 (https://arxiv.org/abs/1803.06882). Bibcode:2018AnHP...19.3321M (https://ui.adsabs.harvard.edu/abs/2018AnHP...19.3321M). doi:10.1007/s00023-018-0729-8 (https://doi.org/10.1007%2Fs00023-018-0729-8). S2CID 53630146 (https://api.semanticscholar.org/CorpusID:53630146).
14. Bell, John (1966). "On the Problem of Hidden Variables in Quantum Mechanics". *Reviews of Modern Physics*. **38** (3): 447. Bibcode:1966RvMP...38..447B (https://ui.adsabs.harvard.edu/abs/1966RvMP...38..447B). doi:10.1103/RevModPhys.38.447 (https://doi.org/10.1103%2FRevModPhys.38.447). OSTI 1444158 (https://www.osti.gov/biblio/1444158).
15. Bub, Jeffrey (2010). "Von Neumann's 'No Hidden Variables' Proof: A Re-Appraisal". *Foundations of Physics*. **40** (9–10): 1333–1340. arXiv:1006.0499 (https://arxiv.org/abs/1006.0499). Bibcode:2010FoPh...40.1333B (https://ui.adsabs.harvard.edu/abs/2010FoPh...40.1333B). doi:10.1007/s10701-010-9480-9 (https://doi.org/10.1007%2Fs10701-010-9480-9). S2CID 118595119 (https://api.semanticscholar.org/CorpusID:118595119).

16. Mermin, N. David; Schack, Rüdiger (2018). "Homer nodded: von Neumann's surprising oversight". *Foundations of Physics*. **48** (9): 1007–1020. arXiv:1805.10311 (https://arxiv.org/abs/1805.10311). Bibcode:2018FoPh...48.1007M (https://ui.adsabs.harvard.edu/abs/2018FoPh...48.1007M). doi:10.1007/s10701-018-0197-5 (https://doi.org/10.1007%2Fs10701-018-0197-5). S2CID 118951033 (https://api.semanticscholar.org/CorpusID:118951033).
17. Peres, Asher (1992). "An experimental test for Gleason's theorem". *Physics Letters A*. **163** (4): 243–245. Bibcode:1992PhLA..163..243P (https://ui.adsabs.harvard.edu/abs/1992PhLA..163..243P). doi:10.1016/0375-9601(92)91005-C (https://doi.org/10.1016%2F0375-9601%2892%2991005-C).
18. Mackey, George W. (1957). "Quantum Mechanics and Hilbert Space". *The American Mathematical Monthly*. **64** (8P2): 45–57. doi:10.1080/00029890.1957.11989120 (https://doi.org/10.1080%2F00029890.1957.11989120). JSTOR 2308516 (https://www.jstor.org/stable/2308516).
19. Chernoff, Paul R. "Andy Gleason and Quantum Mechanics" (https://www.ams.org/notices/200910/rtx091001236p.pdf) (PDF). *Notices of the AMS*. **56** (10): 1253–1259.
20. Hrushovski, Ehud; Pitowsky, Itamar (2004-06-01). "Generalizations of Kochen and Specker's theorem and the effectiveness of Gleason's theorem". *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*. **35** (2): 177–194. arXiv:quant-ph/0307139 (https://arxiv.org/abs/quant-ph/0307139). Bibcode:2004SHPMP..35..177H (https://ui.adsabs.harvard.edu/abs/2004SHPMP..35..177H). doi:10.1016/j.shpsb.2003.10.002 (https://doi.org/10.1016%2Fj.shpsb.2003.10.002). S2CID 15265001 (https://api.semanticscholar.org/CorpusID:15265001).
21. Cooke, Roger; Keane, Michael; Moran, William (1985). "An elementary proof of Gleason's theorem". *Mathematical Proceedings of the Cambridge Philosophical Society*. **98** (1): 117–128. Bibcode:1985MPCPS..98..117C (https://ui.adsabs.harvard.edu/abs/1985MPCPS..98..117C). doi:10.1017/S0305004100063313 (https://doi.org/10.1017%2FS0305004100063313). S2CID 124627182 (https://api.semanticscholar.org/CorpusID:124627182).
22. Pitowsky, Itamar (1998). "Infinite and finite Gleason's theorems and the logic of indeterminacy" (https://doi.org/10.1063%2F1.532334). *Journal of Mathematical Physics*. **39** (1): 218–228. Bibcode:1998JMP....39..218P (https://ui.adsabs.harvard.edu/abs/1998JMP....39..218P). doi:10.1063/1.532334 (https://doi.org/10.1063%2F1.532334).
23. Hudson, Robin Lyth (1986). "Geometry of quantum theory". *The Mathematical Gazette*. **70** (454): 332–333. doi:10.2307/3616230 (https://doi.org/10.2307%2F3616230). JSTOR 3616230 (https://www.jstor.org/stable/3616230).
24. Fuchs, Christopher A. (2011). *Coming of Age with Quantum Information: Notes on a Paulian Idea*. Cambridge: Cambridge University Press. ISBN 978-0-521-19926-1. OCLC 535491156 (https://search.worldcat.org/oclc/535491156).
25. Stairs, Allen (2015). "Quantum Logic and Quantum Reconstruction". *Foundations of Physics*. **45** (10): 1351–1361. arXiv:1501.05492 (https://arxiv.org/abs/1501.05492). Bibcode:2015FoPh...45.1351S (https://ui.adsabs.harvard.edu/abs/2015FoPh...45.1351S). doi:10.1007/s10701-015-9879-4 (https://doi.org/10.1007%2Fs10701-015-9879-4). S2CID 126435 (https://api.semanticscholar.org/CorpusID:126435).
26. Wilce, A. (2021-08-10). "Quantum Logic and Probability Theory" (https://plato.stanford.edu/entries/qt-quantlog/). In Zalta, Edward N. (ed.). *Stanford Encyclopedia of Philosophy* (Spring 2017 ed.).
27. Mermin, N. David (1993-07-01). "Hidden variables and the two theorems of John Bell". *Reviews of Modern Physics*. **65** (3): 803–815. arXiv:1802.10119 (https://arxiv.org/abs/1802.10119). Bibcode:1993RvMP...65..803M (https://ui.adsabs.harvard.edu/abs/1993RvMP...65..803M). doi:10.1103/RevModPhys.65.803 (https://doi.org/10.1103%2FRevModPhys.65.803). S2CID 119546199 (https://api.semanticscholar.org/CorpusID:119546199).

28. Shimony, Abner (1984). "Contextual Hidden Variable Theories and Bell's Inequalities". *British Journal for the Philosophy of Science*. **35** (1): 25–45. doi:10.1093/bjps/35.1.25 (https://doi.org/10.1093%2Fbjps%2F35.1.25).
29. Harrigan, Nicholas; Spekkens, Robert W. (2010). "Einstein, incompleteness, and the epistemic view of quantum states". *Foundations of Physics*. **40** (2): 125–157. arXiv:0706.2661 (https://arxiv.org/abs/0706.2661). Bibcode:2010FoPh...40..125H (https://ui.adsabs.harvard.edu/abs/2010FoPh...40..125H). doi:10.1007/s10701-009-9347-0 (https://doi.org/10.1007%2Fs10701-009-9347-0). S2CID 32755624 (https://api.semanticscholar.org/CorpusID:32755624).
30. Peres, Asher (1991). "Two simple proofs of the Kochen-Specker theorem" (http://stacks.iop.org/0305-4470/24/i=4/a=003). *Journal of Physics A: Mathematical and General*. **24** (4): L175–L178. Bibcode:1991JPhA...24L.175P (https://ui.adsabs.harvard.edu/abs/1991JPhA...24L.175P). doi:10.1088/0305-4470/24/4/003 (https://doi.org/10.1088%2F0305-4470%2F24%2F4%2F003). ISSN 0305-4470 (https://search.worldcat.org/issn/0305-4470).
31. Stairs, Allen (1983). "Quantum Logic, Realism, and Value Definiteness". *Philosophy of Science*. **50** (4): 578–602. doi:10.1086/289140 (https://doi.org/10.1086%2F289140). S2CID 122885859 (https://api.semanticscholar.org/CorpusID:122885859).
32. Heywood, Peter; Redhead, Michael L. G. (1983). "Nonlocality and the Kochen–Specker paradox". *Foundations of Physics*. **13** (5): 481–499. Bibcode:1983FoPh...13..481H (https://ui.adsabs.harvard.edu/abs/1983FoPh...13..481H). doi:10.1007/BF00729511 (https://doi.org/10.1007%2FBF00729511). S2CID 120340929 (https://api.semanticscholar.org/CorpusID:120340929).
33. Edwards, David (1979). "The Mathematical Foundations of Quantum Mechanics". *Synthese*. **42**: 1–70. doi:10.1007/BF00413704 (https://doi.org/10.1007%2FBF00413704). S2CID 46969028 (https://api.semanticscholar.org/CorpusID:46969028).
34. van Fraassen, Bas (1991). *Quantum Mechanics: An Empiricist View* (https://archive.org/details/quantummechanics0000vanf). Clarendon Press. ISBN 9780198239802. OCLC 1005285550 (https://search.worldcat.org/oclc/1005285550).
35. Barad, Karen (2007). *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*. Duke University Press. ISBN 9780822339175. OCLC 894219980 (https://search.worldcat.org/oclc/894219980).
36. Dvurecenskij, Anatolij (1992). *Gleason's Theorem and Its Applications*. Mathematics and its Applications, Vol. 60. Dordrecht: Kluwer Acad. Publ. p. 348. ISBN 978-0-7923-1990-0. OCLC 751579618 (https://search.worldcat.org/oclc/751579618).
37. Baez, John C. (2010-12-01). "Solèr's Theorem" (https://golem.ph.utexas.edu/category/2010/12/solers_theorem.html). *The n-Category Café*. Retrieved 2017-04-24.
38. Moretti, Valter; Oppio, Marco (2019-06-01). "Quantum theory in quaternionic Hilbert space: How Poincaré symmetry reduces the theory to the standard complex one". *Reviews in Mathematical Physics*. **31** (4): 1950013–502. arXiv:1709.09246 (https://arxiv.org/abs/1709.09246). Bibcode:2019RvMaP..3150013M (https://ui.adsabs.harvard.edu/abs/2019RvMaP..3150013M). doi:10.1142/S0129055X19500132 (https://doi.org/10.1142%2FS0129055X19500132). S2CID 119733863 (https://api.semanticscholar.org/CorpusID:119733863).
39. Busch, Paul (2003). "Quantum States and Generalized Observables: A Simple Proof of Gleason's Theorem". *Physical Review Letters*. **91** (12): 120403. arXiv:quant-ph/9909073 (https://arxiv.org/abs/quant-ph/9909073). Bibcode:2003PhRvL..91l0403B (https://ui.adsabs.harvard.edu/abs/2003PhRvL..91l0403B). doi:10.1103/PhysRevLett.91.120403 (https://doi.org/10.1103%2FPhysRevLett.91.120403). PMID 14525351 (https://pubmed.ncbi.nlm.nih.gov/14525351). S2CID 2168715 (https://api.semanticscholar.org/CorpusID:2168715).

40. Caves, Carlton M.; Fuchs, Christopher A.; Manne, Kiran K.; Renes, Joseph M. (2004). "Gleason-Type Derivations of the Quantum Probability Rule for Generalized Measurements". *Foundations of Physics*. **34** (2): 193–209. arXiv:quant-ph/0306179 (https://arxiv.org/abs/quant-ph/0306179). Bibcode:2004FoPh...34..193C (https://ui.adsabs.harvard.edu/abs/2004FoPh...34..193C). doi:10.1023/B:FOOP.0000019581.00318.a5 (https://doi.org/10.1023%2FB%3AFOOP.0000019581.00318.a5). S2CID 18132256 (https://api.semanticscholar.org/CorpusID:18132256).
41. Spekkens, Robert W. (2014). "The Status of Determinism in Proofs of the Impossibility of a Noncontextual Model of Quantum Theory". *Foundations of Physics*. **44** (11): 1125–1155. arXiv:1312.3667 (https://arxiv.org/abs/1312.3667). Bibcode:2014FoPh...44.1125S (https://ui.adsabs.harvard.edu/abs/2014FoPh...44.1125S). doi:10.1007/s10701-014-9833-x (https://doi.org/10.1007%2Fs10701-014-9833-x). S2CID 118469528 (https://api.semanticscholar.org/CorpusID:118469528).
42. Wright, Victoria J.; Weigert, Stephan (2019). "A Gleason-type theorem for qubits based on mixtures of projective measurements". *Journal of Physics A*. **52** (5): 055301. arXiv:1808.08091 (https://arxiv.org/abs/1808.08091). Bibcode:2019JPhA...52e5301W (https://ui.adsabs.harvard.edu/abs/2019JPhA...52e5301W). doi:10.1088/1751-8121/aaf93d (https://doi.org/10.1088%2F1751-8121%2Faaf93d). S2CID 119309162 (https://api.semanticscholar.org/CorpusID:119309162).
43. Grudka, Andrzej; Kurzyński, Paweł (2008). "Is There Contextuality for a Single Qubit?". *Physical Review Letters*. **100** (16): 160401. arXiv:0705.0181 (https://arxiv.org/abs/0705.0181). Bibcode:2008PhRvL.100p0401G (https://ui.adsabs.harvard.edu/abs/2008PhRvL.100p0401G). doi:10.1103/PhysRevLett.100.160401 (https://doi.org/10.1103%2FPhysRevLett.100.160401). PMID 18518167 (https://pubmed.ncbi.nlm.nih.gov/18518167). S2CID 13251108 (https://api.semanticscholar.org/CorpusID:13251108).
44. Richman, Fred; Bridges, Douglas (1999-03-10). "A Constructive Proof of Gleason's Theorem" (https://doi.org/10.1006%2Fjfan.1998.3372). *Journal of Functional Analysis*. **162** (2): 287–312. doi:10.1006/jfan.1998.3372 (https://doi.org/10.1006%2Fjfan.1998.3372). hdl:2292/3547 (https://hdl.handle.net/2292%2F3547).
45. Hamhalter, Jan (2003-10-31). *Quantum Measure Theory* (https://books.google.com/books?id=jU7jzm4PylUC). Springer Science & Business Media. ISBN 9781402017148. MR 2015280 (https://mathscinet.ams.org/mathscinet-getitem?mr=2015280). OCLC 928681664 (https://search.worldcat.org/oclc/928681664). Zbl 1038.81003 (https://zbmath.org/?format=complete&q=an:1038.81003).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Gleason%27s_theorem&oldid=1219005616"

WIKIPEDIA
The Free Encyclopedia

Gottesman–Knill theorem

In quantum computing, the **Gottesman–Knill theorem** is a theoretical result by Daniel Gottesman and Emanuel Knill that states that stabilizer circuits, circuits that only consist of gates from the normalizer of the qubit Pauli group, also called Clifford group, can be perfectly simulated in polynomial time on a probabilistic classical computer. The Clifford group can be generated solely by using CNOT, Hadamard, and phase gate S;[1] and therefore stabilizer circuits can be constructed using only these gates.

The reason for the speed up of quantum computers is not yet fully understood. The theorem proves that, for all quantum algorithms with a speed up that relies on entanglement which can be achieved with a CNOT and a Hadamard gate to produce entangled states, this kind of entanglement alone does not give any computing advantage.

There exists a more efficient simulation of stabilizer circuits than the construction of the original publication[1] with an implementation.[2]

The Gottesman–Knill theorem was published in a single author paper by Gottesman in which he credits Knill with the result through private communication.[3]

Formal statement

Theorem: A quantum circuit using only the following elements can be simulated efficiently on a classical computer:

1. Preparation of qubits in computational basis states,
2. Clifford gates (Hadamard gates, controlled NOT gates, phase gate S), and
3. Measurements in the computational basis.

The Gottesman–Knill theorem shows that even some highly entangled states can be simulated efficiently. Several important types of quantum algorithms use only Clifford gates, most importantly the standard algorithms for entanglement distillation and for quantum error correction. From a practical point of view, stabilizer circuits have been simulated in $O(n \log n)$ time using the graph state formalism.

See also

- Magic state distillation

References

1. Aaronson, Scott; Gottesman, Daniel (2004). "Improved simulation of stabilizer circuits". *Physical Review A*. **70** (5): 052328. arXiv:quant-ph/0406196 (https://arxiv.org/abs/quant-ph/0406196). Bibcode:2004PhRvA..70e2328A (https://ui.adsabs.harvard.edu/abs/2004PhRvA..7

0e2328A). doi:10.1103/physreva.70.052328 (https://doi.org/10.1103%2Fphysreva.70.052328). S2CID 5289248 (https://api.semanticscholar.org/CorpusID:5289248).
2. Aaronson, Scott; Gottesman, Daniel. "CHP: CNOT-Hadamard-Phase" (https://www.scottaaronson.com/chp/). *scottaaronson*. Retrieved 19 September 2017.
3. Gottesman, Daniel (1998). "The Heisenberg Representation of Quantum Computers". arXiv:quant-ph/9807006 (https://arxiv.org/abs/quant-ph/9807006).

- Daniel Gottesman (1998). "The Heisenberg Representation of Quantum Computers". arXiv:quant-ph/9807006 (https://arxiv.org/abs/quant-ph/9807006).
- S. Anders and H. J. Briegel (2006). "Fast simulation of stabilizer circuits using a graph-state representation". *Physical Review A*. **73** (2): 022334. arXiv:quant-ph/0504117v2 (https://arxiv.org/abs/quant-ph/0504117v2). Bibcode:2006PhRvA..73b2334A (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73b2334A). doi:10.1103/PhysRevA.73.022334 (https://doi.org/10.1103%2FPhysRevA.73.022334). S2CID 12763101 (https://api.semanticscholar.org/CorpusID:12763101).
- Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information* (2nd ed.). Cambridge: Cambridge University Press. ISBN 978-1-107-00217-3. OCLC 844974180 (https://search.worldcat.org/oclc/844974180).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Gottesman–Knill_theorem&oldid=1161655335"

WIKIPEDIA
The Free Encyclopedia

Holevo's theorem

Holevo's theorem is an important limitative theorem in quantum computing, an interdisciplinary field of physics and computer science. It is sometimes called **Holevo's bound**, since it establishes an upper bound to the amount of information that can be known about a quantum state (accessible information). It was published by Alexander Holevo in 1973.

Statement of the theorem

Suppose Alice wants to send a classical message to Bob by encoding it into a quantum state, and suppose she can prepare a state from some fixed set $\{\rho_1, \ldots, \rho_n\}$, with the i-th state prepared with probability p_i. Let X be the classical register containing the choice of state made by Alice. Bob's objective is to recover the value of X from measurement results on the state he received. Let Y be the classical register containing Bob's measurement outcome. Note that Y is therefore a random variable whose probability distribution depends on Bob's choice of measurement.

Holevo's theorem bounds the amount of correlation between the classical registers X and Y, regardless of Bob's measurement choice, in terms of the *Holevo information*. This is useful in practice because the Holevo information does not depend on the measurement choice, and therefore its computation does not require performing an optimization over the possible measurements.

More precisely, define the *accessible information* between X and Y as the (classical) mutual information between the two registers maximized over all possible choices of measurements on Bob's side:

$$I_{\text{acc}}(X:Y) = \sup_{\{\Pi_i^B\}_i} I(X:Y|\{\Pi_i^B\}_i),$$

where $I(X:Y|\{\Pi_i^B\}_i)$ is the (classical) mutual information of the joint probability distribution given by $p_{ij} = p_i \operatorname{Tr}(\Pi_j^B \rho_i)$. There is currently no known formula to analytically solve the optimization in the definition of accessible information in the general case. Nonetheless, we always have the upper bound:

$$I_{\text{acc}}(X:Y) \leq \chi(\eta) \equiv S\left(\sum_i p_i \rho_i\right) - \sum_i p_i S(\rho_i),$$

where $\eta \equiv \{(p_i, \rho_i)\}_i$ is the ensemble of states Alice is using to send information, and S is the von Neumann entropy. This $\chi(\eta)$ is called the **Holevo information** or **Holevo χ quantity**.

Note that the Holevo information also equals the quantum mutual information of the classical-quantum state corresponding to the ensemble:

$$\chi(\eta) = I\left(\sum_i p_i |i\rangle\langle i| \otimes \rho_i\right),$$

with $I(\rho_{AB}) \equiv S(\rho_A) + S(\rho_B) - S(\rho_{AB})$ the quantum mutual information of the bipartite state ρ_{AB}. It follows that Holevo's theorem can be concisely summarized as a bound on the accessible information in terms of the quantum mutual information for classical-quantum states.

Proof

Consider the composite system that describes the entire communication process, which involves Alice's classical input X, the quantum system Q, and Bob's classical output Y. The classical input X can be written as a classical register $\rho^X := \sum_{x=1}^n p_x |x\rangle\langle x|$ with respect to some orthonormal basis $\{|x\rangle\}_{x=1}^n$. By writing X in this manner, the von Neumann entropy $S(X)$ of the state ρ^X corresponds to the Shannon entropy $H(X)$ of the probability distribution $\{p_x\}_{x=1}^n$:

$$S(X) = -\operatorname{tr}\left(\rho^X \log \rho^X\right) = -\operatorname{tr}\left(\sum_{x=1}^{n} p_x \log p_x |x\rangle\langle x|\right) = -\sum_{x=1}^{n} p_x \log p_x = H(X).$$

The initial state of the system, where Alice prepares the state ρ_x with probability p_x, is described by

$$\rho^{XQ} := \sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \rho_x.$$

Afterwards, Alice sends the quantum state to Bob. As Bob only has access to the quantum system Q but not the input X, he receives a mixed state of the form $\rho := \operatorname{tr}_X\left(\rho^{XQ}\right) = \sum_{x=1}^{n} p_x \rho_x$. Bob measures this state with respect to the POVM elements $\{E_y\}_{y=1}^{m}$, and the probabilities $\{q_y\}_{y=1}^{m}$ of measuring the outcomes $y = 1, 2, \ldots, m$ form the classical output Y. This measurement process can be described as a quantum instrument

$$\mathcal{E}^Q(\rho_x) = \sum_{y=1}^{m} q_{y|x} \rho_{y|x} \otimes |y\rangle\langle y|,$$

where $q_{y|x} = \operatorname{tr}(E_y \rho_x)$ is the probability of outcome y given the state ρ_x, while $\rho_{y|x} = W\sqrt{E_y}\rho_x\sqrt{E_y}W^\dagger / q_{y|x}$ for some unitary W is the normalised post-measurement state. Then, the state of the entire system after the measurement process is

$$\rho^{XQ'Y} := \left[\mathcal{I}^X \otimes \mathcal{E}^Q\right]\left(\rho^{XQ}\right) = \sum_{x=1}^{n}\sum_{y=1}^{m} p_x q_{y|x} |x\rangle\langle x| \otimes \rho_{y|x} \otimes |y\rangle\langle y|.$$

Here $\mathcal{I}^X$ is the identity channel on the system X. Since $\mathcal{E}^Q$ is a quantum channel, and the quantum mutual information is monotonic under completely positive trace-preserving maps,[1] $S(X:Q'Y) \leq S(X:Q)$. Additionally, as the partial trace over Q' is also completely positive and trace-preserving, $S(X:Y) \leq S(X:Q'Y)$. These two inequalities give

$$S(X:Y) \leq S(X:Q).$$

On the left-hand side, the quantities of interest depend only on

$$\rho^{XY} := \operatorname{tr}_{Q'}\left(\rho^{XQ'Y}\right) = \sum_{x=1}^{n}\sum_{y=1}^{m} p_x q_{y|x} |x\rangle\langle x| \otimes |y\rangle\langle y| = \sum_{x=1}^{n}\sum_{y=1}^{m} p_{x,y} |x,y\rangle\langle x,y|,$$

with joint probabilities $p_{x,y} = p_x q_{y|x}$. Clearly, ρ^{XY} and $\rho^Y := \operatorname{tr}_X(\rho^{XY})$, which are in the same form as ρ^X, describe classical registers. Hence,

$$S(X:Y) = S(X) + S(Y) - S(XY) = H(X) + H(Y) - H(XY) = I(X:Y).$$

Meanwhile, $S(X:Q)$ depends on the term

$$\log \rho^{XQ} = \log\left(\sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \rho_x\right) = \sum_{x=1}^{n} |x\rangle\langle x| \otimes \log(p_x \rho_x) = \sum_{x=1}^{n} \log p_x |x\rangle\langle x| \otimes I^Q + \sum_{x=1}^{n} |x\rangle\langle x| \otimes \log \rho_x,$$

where I^Q is the identity operator on the quantum system Q. Then, the right-hand side is

$$
\begin{aligned}
S(X:Q) &= S(X) + S(Q) - S(XQ) \\
&= S(X) + S(\rho) + \operatorname{tr}\left(\rho^{XQ} \log \rho^{XQ}\right) \\
&= S(X) + S(\rho) + \operatorname{tr}\left(\sum_{x=1}^{n} p_x \log p_x |x\rangle\langle x| \otimes \rho_x\right) + \operatorname{tr}\left(\sum_{x=1}^{n} p_x |x\rangle\langle x| \otimes \rho_x \log \rho_x\right) \\
&= S(X) + S(\rho) + \underbrace{\operatorname{tr}\left(\sum_{x=1}^{n} p_x \log p_x |x\rangle\langle x|\right)}_{-S(X)} + \operatorname{tr}\left(\sum_{x=1}^{n} p_x \rho_x \log \rho_x\right) \\
&= S(\rho) + \sum_{x=1}^{n} p_x \underbrace{\operatorname{tr}(\rho_x \log \rho_x)}_{-S(\rho_x)} \\
&= S(\rho) - \sum_{x=1}^{n} p_x S(\rho_x),
\end{aligned}
$$

which completes the proof.

Comments and remarks

In essence, the Holevo bound proves that given *n* qubits, although they can "carry" a larger amount of (classical) information (thanks to quantum superposition), the amount of classical information that can be *retrieved*, i.e. *accessed*, can be only up to *n* classical (non-quantum encoded) bits. It was also established, both theoretically and experimentally, that there are computations where quantum bits carry more information through the process of the computation than is possible classically.[2]

See also

- Superdense coding

References

1. Preskill, John (June 2016). "Chapter 10. Quantum Shannon Theory" (https://authors.library.caltech.edu/6649 3/2/chap10_15.pdf) (PDF). *Quantum Information*. pp. 23–24. Retrieved 30 June 2021.
2. Maslov, Dmitri; Kim, Jin-Sung; Bravyi, Sergey; Yoder, Theodore J.; Sheldon, Sarah (2021-06-28). "Quantum advantage for computations with limited space". *Nature Physics*. **17** (8): 894–897. arXiv:2008.06478 (https://arxiv.org/abs/2008.06478). Bibcode:2021NatPh..17..894M (https://ui.adsabs.harvard.edu/abs/2021NatPh..17..894M). doi:10.1038/s41567-021-01271-7 (https://doi.org/10.1038%2Fs41567-021-01271-7). S2CID 221136153 (https://api.semanticscholar.org/CorpusID:221136153).

Further reading

- Holevo, Alexander S. (1973). "Bounds for the quantity of information transmitted by a quantum communication channel". *Problems of Information Transmission*. **9**: 177–183.
- Nielsen, Michael A.; Chuang, Isaac L. (2000). *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press. ISBN 978-0-521-63235-5. OCLC 43641333 (https://search.worldcat.org/oclc/43641333). (see page 531, subsection 12.1.1 - equation (12.6))
- Wilde, Mark M. (2011). "From Classical to Quantum Shannon Theory". arXiv:1106.1445v2 (https://arxiv.org/abs/1106.1445v2) [quant-ph (https://arxiv.org/archive/quant-ph)].. See in particular Section 11.6 and following. Holevo's theorem is presented as exercise 11.9.1 on page 288.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Holevo%27s_theorem&oldid=1223170967"

WIKIPEDIA
The Free Encyclopedia

No-broadcasting theorem

In physics, the **no-broadcasting theorem** is a result of quantum information theory. In the case of pure quantum states, it is a corollary of the no-cloning theorem. The no-cloning theorem for pure states says that it is impossible to create two copies of an unknown state given a single copy of the state. Since quantum states cannot be copied in general, they cannot be broadcast. Here, the word "broadcast" is used in the sense of conveying the state to two or more recipients. For multiple recipients to each receive the state, there must be, in some sense, a way of duplicating the state. The no-broadcast theorem generalizes the no-cloning theorem for mixed states.

The theorem[1] also includes a converse: if two quantum states do commute, there is a method for broadcasting them: they must have a common basis of eigenstates diagonalizing them simultaneously, and the map that clones every state of this basis is a legitimate quantum operation, requiring only physical resources independent of the input state to implement—a completely positive map. A corollary is that there is a physical process capable of broadcasting every state in some set of quantum states if, and only if, every pair of states in the set commutes. This broadcasting map, which works in the commuting case, produces an overall state in which the two copies are perfectly correlated in their eigenbasis.

Remarkably, the theorem does not hold if more than one copy of the initial state is provided: for example, broadcasting six copies starting from four copies of the original state is allowed, even if the states are drawn from a non-commuting set. The purity of the state can even be increased in the process, a phenomenon known as superbroadcasting.[2]

Generalized No-Broadcast Theorem

The generalized quantum no-broadcasting theorem, originally proven by Barnum, Caves, Fuchs, Jozsa and Schumacher for mixed states of finite-dimensional quantum systems,[1] says that given a pair of quantum states which do not commute, there is no method capable of taking a single copy of either state and succeeding, no matter which state was supplied and without incorporating knowledge of which state has been supplied, in producing a state such that one part of it is the same as the original state and the other part is also the same as the original state. That is, given an initial unknown state ρ_i, drawn from the set $\{\rho_i\}_{i\in\{1,2\}}$ such that $[\rho_1, \rho_2] \neq 0$, there is no process (using physical means independent of those used to select the state) guaranteed to create a state ρ_{AB} in a Hilbert space $H_A \otimes H_B$ whose partial traces are $\mathrm{Tr}_A\, \rho_{AB} = \rho_i$ and $\mathrm{Tr}_B\, \rho_{AB} = \rho_i$. Such a process was termed broadcasting in that paper.

No-Local-Broadcasting Theorem

The second theorem states that local broadcasting is only possible when the state is a classical probability distribution.[3] This means that a state can only be broadcast locally if it does not have any quantum correlations.[4] Luo reconciled this theorem with the generalized no-broadcast theorem by making the conjecture that when a state is a classical-quantum state, correlations (rather than the state itself) in a

bipartite state can be locally broadcast.[3] By mathematically proving that his conjecture and the two theorems all relate to and imply one another, Luo proved that all three statements are logically equivalent.[3]

See also

- No-communication theorem
- No-hiding theorem[5]
- Quantum teleportation
- Quantum entanglement
- Quantum information
- Uncertainty principle

References

1. Barnum, Howard; Caves, Carlton M.; Fuchs, Christopher A.; Jozsa, Richard; Schumacher, Benjamin (1996-04-08). "Noncommuting Mixed States Cannot Be Broadcast". *Physical Review Letters*. **76** (15): 2818–2821. arXiv:quant-ph/9511010 (https://arxiv.org/abs/quant-ph/9511010). Bibcode:1996PhRvL..76.2818B (https://ui.adsabs.harvard.edu/abs/1996PhRvL..76.2818B). doi:10.1103/physrevlett.76.2818 (https://doi.org/10.1103%2Fphysrevlett.76.2818). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10060796 (https://pubmed.ncbi.nlm.nih.gov/10060796). S2CID 11724387 (https://api.semanticscholar.org/CorpusID:11724387).
2. D'Ariano, Giacomo Mauro; Macchiavello, Chiara; Perinotti, Paolo (2005-08-05). "Superbroadcasting of Mixed States". *Physical Review Letters*. **95** (6): 060503. arXiv:quant-ph/0506251 (https://arxiv.org/abs/quant-ph/0506251). Bibcode:2005PhRvL..95f0503D (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95f0503D). doi:10.1103/physrevlett.95.060503 (https://doi.org/10.1103%2Fphysrevlett.95.060503). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 16090933 (https://pubmed.ncbi.nlm.nih.gov/16090933). S2CID 2978617 (https://api.semanticscholar.org/CorpusID:2978617).
3. Luo, Shunlong (2010). "On Quantum No-Broadcasting" (https://link.springer.com/epdf/10.1007/s11005-010-0389-1?sharing_token=iszqKKtl5PQn3Z3o0zzRLPe4RwlQNchNByi7wbcMAY53B3x3PD8d78OwZ1RAR8IktfDHbO4kZZAlLYQo0rTfpOREIlcwn70lG7uJgloU3FZCk1WuqJypS1OeKfwtC4qZSy829VxKRMTbGa5-bBMKpu0QHf2tdNsCMlZGO7K1I60%3D). *Letters in Mathematical Physics*. **92** (2): 143–153. Bibcode:2010LMaPh..92..143L (https://ui.adsabs.harvard.edu/abs/2010LMaPh..92..143L). doi:10.1007/s11005-010-0389-1 (https://doi.org/10.1007%2Fs11005-010-0389-1). S2CID 121819242 (https://api.semanticscholar.org/CorpusID:121819242). Retrieved 2020-10-16.
4. Piani, Marco; Horodecki, Pawel; Horodecki, Ryszard (2008-03-06). "No-local-broadcasting theorem for quantum correlations". *Physical Review Letters*. **100** (9): 090502. arXiv:0707.0848 (https://arxiv.org/abs/0707.0848). doi:10.1103/PhysRevLett.100.090502 (https://doi.org/10.1103%2FPhysRevLett.100.090502). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 18352686 (https://pubmed.ncbi.nlm.nih.gov/18352686). S2CID 42381925 (https://api.semanticscholar.org/CorpusID:42381925).
5. Quantum no-hiding theorem experimentally confirmed for first time (http://phys.org/news/2011-03-quantum-no-hiding-theorem-experimentally.html). Mar 07, 2011 by Lisa Zyga.

Retrieved from "https://en.wikipedia.org/w/index.php?title=No-broadcasting_theorem&oldid=1160885931"

WIKIPEDIA
The Free Encyclopedia

No-cloning theorem

In physics, the **no-cloning theorem** states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state, a statement which has profound implications in the field of quantum computing among others. The theorem is an evolution of the 1970 no-go theorem authored by James Park,[1] in which he demonstrates that a non-disturbing measurement scheme which is both simple and perfect cannot exist (the same result would be independently derived in 1982 by William Wootters and Wojciech H. Zurek[2] as well as Dennis Dieks[3] the same year). The aforementioned theorems do not preclude the state of one system becoming entangled with the state of another as cloning specifically refers to the creation of a separable state with identical factors. For example, one might use the controlled NOT gate and the Walsh–Hadamard gate to entangle two qubits without violating the no-cloning theorem as no well-defined state may be defined in terms of a subsystem of an entangled state. The no-cloning theorem (as generally understood) concerns only pure states whereas the generalized statement regarding mixed states is known as the no-broadcast theorem.

The no-cloning theorem has a time-reversed dual, the no-deleting theorem. Together, these underpin the interpretation of quantum mechanics in terms of category theory, and, in particular, as a dagger compact category.[4][5] This formulation, known as categorical quantum mechanics, allows, in turn, a connection to be made from quantum mechanics to linear logic as the logic of quantum information theory (in the same sense that intuitionistic logic arises from Cartesian closed categories).

History

According to Asher Peres[6] and David Kaiser,[7] the publication of the 1982 proof of the no-cloning theorem by Wootters and Zurek[2] and by Dieks[3] was prompted by a proposal of Nick Herbert[8] for a superluminal communication device using quantum entanglement, and Giancarlo Ghirardi[9] had proven the theorem 18 months prior to the published proof by Wootters and Zurek in his referee report to said proposal (as evidenced by a letter from the editor[9]). However, Juan Ortigoso[10] pointed out in 2018 that a complete proof along with an interpretation in terms of the lack of simple nondisturbing measurements in quantum mechanics was already delivered by Park in 1970.[1]

Theorem and proof

Suppose we have two quantum systems *A* and *B* with a common Hilbert space $\boldsymbol{H = H_A = H_B}$. Suppose we want to have a procedure to copy the state $|\boldsymbol{\phi}\rangle_{\boldsymbol{A}}$ of quantum system *A*, over the state $|\boldsymbol{e}\rangle_{\boldsymbol{B}}$ of quantum system *B*, for any original state $|\boldsymbol{\phi}\rangle_{\boldsymbol{A}}$ (see bra–ket notation). That is, beginning with the state $|\boldsymbol{\phi}\rangle_{\boldsymbol{A}} \otimes |\boldsymbol{e}\rangle_{\boldsymbol{B}}$, we want to end up with the state $|\boldsymbol{\phi}\rangle_{\boldsymbol{A}} \otimes |\boldsymbol{\phi}\rangle_{\boldsymbol{B}}$. To make a "copy" of the state *A*, we combine it with system *B* in some unknown initial, or blank, state $|\boldsymbol{e}\rangle_{\boldsymbol{B}}$ independent of $|\boldsymbol{\phi}\rangle_{\boldsymbol{A}}$, of which we have no prior knowledge.

The state of the initial composite system is then described by the following tensor product:

$$|\boldsymbol{\phi}\rangle_{\boldsymbol{A}} \otimes |\boldsymbol{e}\rangle_{\boldsymbol{B}}.$$

(in the following we will omit the ⊗ symbol and keep it implicit).

There are only two permissible quantum operations with which we may manipulate the composite system:

- We can perform an observation, which irreversibly collapses the system into some eigenstate of an observable, corrupting the information contained in the qubit(s). This is obviously not what we want.
- Alternatively, we could control the Hamiltonian of the *combined* system, and thus the time-evolution operator *U*(*t*), e.g. for a time-independent Hamiltonian, $\boldsymbol{U(t) = e^{-iHt/\hbar}}$. Evolving up to some fixed time $\boldsymbol{t_0}$ yields a unitary operator *U* on $\boldsymbol{H \otimes H}$, the Hilbert space of the combined system. However, no such unitary operator *U* can clone all states.

The no-cloning theorem answers the following question in the negative: Is it possible to construct a unitary operator *U*, acting on $\boldsymbol{H_A \otimes H_B = H \otimes H}$, under which the state the system B is in always evolves into the state the system A is in, *regardless* of the state system A is in?

Theorem — There is no unitary operator U on $H \otimes H$ such that for all normalised states $|\phi\rangle_A$ and $|e\rangle_B$ in H

$$U(|\phi\rangle_A|e\rangle_B) = e^{i\alpha(\phi,e)}|\phi\rangle_A|\phi\rangle_B$$

for some real number α depending on ϕ and e.

The extra phase factor expresses the fact that a quantum-mechanical state defines a normalised vector in Hilbert space only up to a phase factor i.e. as an element of projectivised Hilbert space.

To prove the theorem, we select an arbitrary pair of states $|\phi\rangle_A$ and $|\psi\rangle_A$ in the Hilbert space H. Because U is supposed to be unitary, we would have

$$\langle\phi|\psi\rangle\langle e|e\rangle \equiv \langle\phi|_A\langle e|_B|\psi\rangle_A|e\rangle_B = \langle\phi|_A\langle e|_B U^\dagger U|\psi\rangle_A|e\rangle_B = e^{-i(\alpha(\phi,e)-\alpha(\psi,e))}\langle\phi|_A\langle\phi|_B|\psi\rangle_A|\psi\rangle_B \equiv e^{-i(\alpha(\phi,e)-\alpha(\psi,e))}\langle\phi|\psi\rangle^2.$$

Since the quantum state $|e\rangle$ is assumed to be normalized, we thus get

$$|\langle\phi|\psi\rangle|^2 = |\langle\phi|\psi\rangle|.$$

This implies that either $|\langle\phi|\psi\rangle| = 1$ or $|\langle\phi|\psi\rangle| = 0$. Hence by the Cauchy–Schwarz inequality either $|\phi\rangle = e^{i\beta}|\psi\rangle$ or $|\phi\rangle$ is orthogonal to $|\psi\rangle$. However, this cannot be the case for two *arbitrary* states. Therefore, a single universal U cannot clone a *general* quantum state. This proves the no-cloning theorem.

Take a qubit for example. It can be represented by two complex numbers, called probability amplitudes (normalised to 1), that is three real numbers (two polar angles and one radius). Copying three numbers on a classical computer using any copy and paste operation is trivial (up to a finite precision) but the problem manifests if the qubit is unitarily transformed (e.g. by the Hadamard quantum gate) to be polarised (which unitary transformation is a surjective isometry). In such a case the qubit can be represented by just two real numbers (one polar angle and one radius equal to 1), while the value of the third can be arbitrary in such a representation. Yet a realisation of a qubit (polarisation-encoded photon, for example) is capable of storing the whole qubit information support within its "structure". Thus no single universal unitary evolution U can clone an arbitrary quantum state according to the no-cloning theorem. It would have to depend on the transformed qubit (initial) state and thus would not have been *universal*.

Generalization

In the statement of the theorem, two assumptions were made: the state to be copied is a pure state and the proposed copier acts via unitary time evolution. These assumptions cause no loss of generality. If the state to be copied is a mixed state, it can be "purified," i.e. treated as a pure state of a larger system. Alternately, a different proof can be given that works directly with mixed states; in this case, the theorem is often known as the no-broadcast theorem.[11][12] Similarly, an arbitrary quantum operation can be implemented via introducing an ancilla and performing a suitable unitary evolution. Thus the no-cloning theorem holds in full generality.

For extensions of quantum computers, no-cloning theorem remains valid if using postselection or two-way quantum computers.[13] However, adding closed timelike curve is claimed to allow to clone quantum state. [14]

Consequences

- The no-cloning theorem prevents the use of certain classical error correction techniques on quantum states. For example, backup copies of a state in the middle of a quantum computation cannot be created and used for correcting subsequent errors. Error correction is vital for practical quantum computing, and for some time it was unclear whether or not it was possible. In 1995, Shor and Steane showed that it is, by independently devising the first quantum error correcting codes, which circumvent the no-cloning theorem.
- Similarly, cloning would violate the no-teleportation theorem, which says that it is impossible to convert a quantum state into a sequence of classical bits (even an infinite sequence of bits), copy those bits to some new location, and recreate a copy of the original quantum state in the new location. This should not be confused with entanglement-assisted teleportation, which does allow a quantum state to be destroyed in one location, and an exact copy to be recreated in another location.
- The no-cloning theorem is implied by the no-communication theorem, which states that quantum entanglement cannot be used to transmit classical information (whether superluminally, or slower). That is, cloning, together with entanglement, would allow such communication to occur. To see this, consider the EPR thought experiment, and suppose quantum states could be cloned. Assume parts of a maximally entangled Bell state are distributed to Alice and Bob. Alice could send bits to Bob in the following way: If Alice wishes to transmit a "0", she measures the spin of her electron in the **z** direction, collapsing Bob's state to either $|z+\rangle_B$ or $|z-\rangle_B$. To transmit "1", Alice does nothing to her qubit. Bob creates many copies of his electron's state, and measures the spin of each copy in the **z** direction. Bob will know that Alice has transmitted a "0" if all his measurements produce the same result; otherwise, his measurements

will have outcomes $|z+\rangle_B$ or $|z-\rangle_B$ with equal probability. This would allow Alice and Bob to communicate classical bits between each other (possibly across space-like separations, violating causality).

- Quantum states cannot be discriminated perfectly.[15]
- The no cloning theorem prevents an interpretation of the holographic principle for black holes as meaning that there are two copies of information, one lying at the event horizon and the other in the black hole interior. This leads to more radical interpretations, such as black hole complementarity.
- The no-cloning theorem applies to all dagger compact categories: there is no universal cloning morphism for any non-trivial category of this kind.[16] Although the theorem is inherent in the definition of this category, it is not trivial to see that this is so; the insight is important, as this category includes things that are not finite-dimensional Hilbert spaces, including the category of sets and relations and the category of cobordisms.

Imperfect cloning

Even though it is impossible to make perfect copies of an unknown quantum state, it is possible to produce imperfect copies. This can be done by coupling a larger auxiliary system to the system that is to be cloned, and applying a unitary transformation to the combined system. If the unitary transformation is chosen correctly, several components of the combined system will evolve into approximate copies of the original system. In 1996, V. Buzek and M. Hillery showed that a universal cloning machine can make a clone of an unknown state with the surprisingly high fidelity of 5/6.[17]

Imperfect quantum cloning can be used as an eavesdropping attack on quantum cryptography protocols, among other uses in quantum information science.

See also

- Fundamental Fysiks Group
- Monogamy of entanglement
- No-broadcast theorem
- No-communication theorem
- No-deleting theorem
- No-hiding theorem
- Quantum entanglement
- Quantum cloning
- Quantum information
- Quantum teleportation
- Stronger uncertainty relations
- Uncertainty principle

References

1. Park, James (1970). "The concept of transition in quantum mechanics". *Foundations of Physics*. **1** (1): 23–33. Bibcode:1970FoPh....1...23P (https://ui.adsabs.harvard.edu/abs/1970FoPh....1...23P). CiteSeerX 10.1.1.623.5267 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.623.5267). doi:10.1007/BF00708652 (https://doi.org/10.1007%2FBF00708652). S2CID 55890485 (https://api.semanticscholar.org/CorpusID:55890485).
2. Wootters, William; Zurek, Wojciech (1982). "A Single Quantum Cannot be Cloned". *Nature*. **299** (5886): 802–803. Bibcode:1982Natur.299..802W (https://ui.adsabs.harvard.edu/abs/1982Natur.299..802W). doi:10.1038/299802a0 (https://doi.org/10.1038%2F299802a0). S2CID 4339227 (https://api.semanticscholar.org/CorpusID:4339227).
3. Dieks, Dennis (1982). "Communication by EPR devices". *Physics Letters A*. **92** (6): 271–272. Bibcode:1982PhLA...92..271D (https://ui.adsabs.harvard.edu/abs/1982PhLA...92..271D). CiteSeerX 10.1.1.654.7183 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.654.7183). doi:10.1016/0375-9601(82)90084-6 (https://doi.org/10.1016%2F0375-9601%2882%2990084-6). hdl:1874/16932 (https://hdl.handle.net/1874%2F16932).
4. Baez, John; Stay, Mike (2010). "Physics, Topology, Logic and Computation: A Rosetta Stone" (http://math.ucr.edu/home/baez/rosetta.pdf) (PDF). *New Structures for Physics*. Berlin: Springer. pp. 95–172. ISBN 978-3-642-12821-9.
5. Coecke, Bob (2009). "Quantum Picturalism". *Contemporary Physics*. **51**: 59–83. arXiv:0908.1787 (https://arxiv.org/abs/0908.1787). doi:10.1080/00107510903257624 (https://doi.org/10.1080%2F00107510903257624). S2CID 752173 (https://api.semanticscholar.org/CorpusID:752173).
6. Peres, Asher (2003). "How the No-Cloning Theorem Got its Name". *Fortschritte der Physik*. **51** (45): 458–461. arXiv:quant-ph/0205076 (https://arxiv.org/abs/quant-ph/0205076). Bibcode:2003ForPh..51..458P (https://ui.adsabs.harvard.edu/abs/2003ForPh..51..458P). doi:10.1002/prop.200310062 (https://doi.org/10.1002%2Fprop.200310062). S2CID 16588882 (https://api.semanticscholar.org/CorpusID:16588882).
7. Kaiser, David (2011). *How the Hippies Saved Physics: Science, Counterculture, and the Quantum Revival*. W. W. Norton. ISBN 978-0-393-07636-3.
8. Herbert, Nick (1982). "FLASH—A superluminal communicator based upon a new kind of quantum measurement". *Foundations of Physics*. **12** (12): 1171–1179. Bibcode:1982FoPh...12.1171H (https://ui.adsabs.harvard.edu/abs/1982FoPh...12.1171H). doi:10.1007/BF00729622 (https://doi.org/10.1007%2FBF00729622). S2CID 123118337 (https://api.semanticscholar.org/CorpusID:123118337).

9. Ghirardi, GianCarlo (2013), "Entanglement, Nonlocality, Superluminal Signaling and Cloning", in Bracken, Paul (ed.), *Advances in Quantum Mechanics*, IntechOpen (published April 3, 2013), arXiv:1305.2305 (https://arxiv.org/abs/1305.2305), doi:10.5772/56429 (https://doi.org/10.5772%2F56429), ISBN 978-953-51-1089-7, S2CID 118778014 (https://api.semanticscholar.org/CorpusID:118778014)
10. Ortigoso, Juan (2018). "Twelve years before the quantum no-cloning theorem". *American Journal of Physics*. **86** (3): 201–205. arXiv:1707.06910 (https://arxiv.org/abs/1707.06910). Bibcode:2018AmJPh..86..201O (https://ui.adsabs.harvard.edu/abs/2018AmJPh..86..201O). doi:10.1119/1.5021356 (https://doi.org/10.1119%2F1.5021356). S2CID 119192142 (https://api.semanticscholar.org/CorpusID:119192142).
11. Barnum, Howard; Caves, Carlton M.; Fuchs, Christopher A.; Jozsa, Richard; Schumacher, Benjamin (1996-04-08). "Noncommuting Mixed States Cannot Be Broadcast". *Physical Review Letters*. **76** (15): 2818–2821. arXiv:quant-ph/9511010 (https://arxiv.org/abs/quant-ph/9511010). Bibcode:1996PhRvL..76.2818B (https://ui.adsabs.harvard.edu/abs/1996PhRvL..76.2818B). doi:10.1103/PhysRevLett.76.2818 (https://doi.org/10.1103%2FPhysRevLett.76.2818). PMID 10060796 (https://pubmed.ncbi.nlm.nih.gov/10060796). S2CID 11724387 (https://api.semanticscholar.org/CorpusID:11724387).
12. Kalev, Amir; Hen, Itay (2008-05-29). "No-Broadcasting Theorem and Its Classical Counterpart". *Physical Review Letters*. **100** (21): 210502. arXiv:0704.1754 (https://arxiv.org/abs/0704.1754). Bibcode:2008PhRvL.100u0502K (https://ui.adsabs.harvard.edu/abs/2008PhRvL.100u0502K). doi:10.1103/PhysRevLett.100.210502 (https://doi.org/10.1103%2FPhysRevLett.100.210502). PMID 18518590 (https://pubmed.ncbi.nlm.nih.gov/18518590). S2CID 40349990 (https://api.semanticscholar.org/CorpusID:40349990).
13. Noor, Mah; Duda, Jarek (2024). "No-cloning theorem for 2WQC and postselection". arXiv:2407.15623 (https://arxiv.org/abs/2407.15623) [quant-ph (https://arxiv.org/archive/quant-ph)].
14. Ahn, Doyeol; Myers, Casey; Ralph, Timothy; Mann, Robert (2013). "Quantum-state cloning in the presence of a closed timelike curve". *Physical Review A*. **88** (2). arXiv:1207.6062 (https://arxiv.org/abs/1207.6062). doi:10.1103/PhysRevA.88.022332 (https://doi.org/10.1103%2FPhysRevA.88.022332).
15. Bae, Joonwoo; Kwek, Leong-Chuan (2015-02-27). "Quantum state discrimination and its applications" (https://iopscience.iop.org/article/10.1088/1751-8113/48/8/083001). *Journal of Physics A: Mathematical and Theoretical*. **48** (8): 083001. arXiv:1707.02571 (https://arxiv.org/abs/1707.02571). Bibcode:2015JPhA...48h3001B (https://ui.adsabs.harvard.edu/abs/2015JPhA...48h3001B). doi:10.1088/1751-8113/48/8/083001 (https://doi.org/10.1088%2F1751-8113%2F48%2F8%2F083001). ISSN 1751-8113 (https://search.worldcat.org/issn/1751-8113). S2CID 119199057 (https://api.semanticscholar.org/CorpusID:119199057).
16. S. Abramsky, "No-Cloning in categorical quantum mechanics", (2008) *Semantic Techniques for Quantum Computation*, I. Mackie and S. Gay (eds), Cambridge University Press. arXiv:0910.2401 (https://arxiv.org/abs/0910.2401)
17. Bužek, V.; Hillery, M. (1996). "Quantum Copying: Beyond the No-Cloning Theorem". *Phys. Rev. A*. **54** (3): 1844–1852. arXiv:quant-ph/9607018 (https://arxiv.org/abs/quant-ph/9607018). Bibcode:1996PhRvA..54.1844B (https://ui.adsabs.harvard.edu/abs/1996PhRvA..54.1844B). doi:10.1103/PhysRevA.54.1844 (https://doi.org/10.1103%2FPhysRevA.54.1844). PMID 9913670 (https://pubmed.ncbi.nlm.nih.gov/9913670). S2CID 1446565 (https://api.semanticscholar.org/CorpusID:1446565).

Other sources

- V. Buzek and M. Hillery, *Quantum cloning*, Physics World 14 (11) (2001), pp. 25–29.

Retrieved from "https://en.wikipedia.org/w/index.php?title=No-cloning_theorem&oldid=1236209149"

WIKIPEDIA
The Free Encyclopedia

No-communication theorem

In physics, the **no-communication theorem** or **no-signaling principle** is a no-go theorem from quantum information theory which states that, during measurement of an entangled quantum state, it is not possible for one observer, by making a measurement of a subsystem of the total state, to communicate information to another observer. The theorem is important because, in quantum mechanics, quantum entanglement is an effect by which certain widely separated events can be correlated in ways that, at first glance, suggest the possibility of communication faster-than-light. The no-communication theorem gives conditions under which such transfer of information between two observers is impossible. These results can be applied to understand the so-called paradoxes in quantum mechanics, such as the EPR paradox, or violations of local realism obtained in tests of Bell's theorem. In these experiments, the no-communication theorem shows that failure of local realism does not lead to what could be referred to as "spooky communication at a distance" (in analogy with Einstein's labeling of quantum entanglement as requiring "spooky action at a distance" on the assumption of QM's completeness).

Informal overview

The no-communication theorem states that, within the context of quantum mechanics, it is not possible to transmit classical bits of information by means of carefully prepared mixed or pure states, whether entangled or not. The theorem is only a sufficient condition that states that if the Kraus matrices commute then there can be no communication through the quantum entangled states and this is applicable to all communication. From a relativity and quantum field perspective also faster than light or "instantaneous" communication is disallowed.[1] Being only a sufficient condition there can be extra cases where communication is not allowed and there can be also cases where is still possible to communicate through the quantum channel encoding more than the classical information.

In regards to communication, a quantum channel can always be used to transfer classical information by means of shared quantum states.[2][3] In 2008 Matthew Hastings proved a counterexample where the minimum output entropy is not additive for all quantum channels. Therefore, by an equivalence result due to Peter Shor,[4] the Holevo capacity is not just additive, but super-additive like the entropy, and by consequence there may be some quantum channels where you can transfer more than the classical capacity.[5][6] Typically overall communication happens at the same time via quantum and non quantum channels, and in general time ordering and causality cannot be violated.

The basic assumption entering into the theorem is that a quantum-mechanical system is prepared in an initial state with some entangled states, and that this initial state is describable as a mixed or pure state in a Hilbert space *H*. After a certain amount of time the system is divided in two parts each of which contains some non entangled states and half of quantum entangled states and the two parts becomes spatially distinct, *A* and *B*, sent to two distinct observers, Alice and Bob, who are free to perform quantum mechanical measurements on their portion of the total system (viz, A and B). The question is: is there any action that Alice can perform on A that would be detectable by Bob making an observation of B? The theorem replies 'no'.

An important assumption going into the theorem is that neither Alice nor Bob is allowed, in any way, to affect the preparation of the initial state. If Alice were allowed to take part in the preparation of the initial state, it would be trivially easy for her to encode a message into it; thus neither Alice nor Bob participates in the preparation of the initial state. The theorem does not require that the initial state be somehow 'random' or 'balanced' or 'uniform': indeed, a third party preparing the initial state could easily encode messages in it, received by Alice and Bob. Simply, the theorem states that, given some initial state, prepared in some way, there is no action that Alice can take that would be detectable by Bob.

The proof proceeds by defining how the total Hilbert space H can be split into two parts, H_A and H_B, describing the subspaces accessible to Alice and Bob. The total state of the system is assumed to be described by a density matrix σ. This appears to be a reasonable assumption, as a density matrix is sufficient to describe both pure and mixed states in quantum mechanics. Another important part of the theorem is that measurement is performed by applying a generalized projection operator P to the state σ. This again is reasonable, as projection operators give the appropriate mathematical description of quantum measurements. After a measurement by Alice, the state of the total system is said to have *collapsed* to a state $P(\sigma)$.

The goal of the theorem is to prove that Bob cannot in any way distinguish the pre-measurement state σ from the post-measurement state $P(\sigma)$. This is accomplished mathematically by comparing the trace of σ and the trace of $P(\sigma)$, with the trace being taken over the subspace H_A. Since the trace is only over a subspace, it is technically called a partial trace. Key to this step is the assumption that the (partial) trace adequately summarizes the system from Bob's point of view. That is, everything that Bob has access to, or could ever have access to, measure, or detect, is completely described by a partial trace over H_A of the system σ. Again, this is a reasonable assumption, as it is a part of standard quantum mechanics. The fact that this trace never changes as Alice performs her measurements is the conclusion of the proof of the no-communication theorem.

Formulation

The proof of the theorem is commonly illustrated for the setup of Bell tests in which two observers Alice and Bob perform local observations on a common bipartite system, and uses the statistical machinery of quantum mechanics, namely density states and quantum operations.[1][7][8]

Alice and Bob perform measurements on system **S** whose underlying Hilbert space is

$$H = H_A \otimes H_B.$$

It is also assumed that everything is finite-dimensional to avoid convergence issues. The state of the composite system is given by a density operator on H. Any density operator σ on H is a sum of the form:

$$\sigma = \sum_i T_i \otimes S_i$$

where T_i and S_i are operators on H_A and H_B respectively. For the following, it is not required to assume that T_i and S_i are state projection operators: *i.e.* they need not necessarily be non-negative, nor have a trace of one. That is, σ can have a definition somewhat broader than that of a density matrix; the theorem

still holds. Note that the theorem holds trivially for separable states. If the shared state σ is separable, it is clear that any local operation by Alice will leave Bob's system intact. Thus the point of the theorem is no communication can be achieved via a shared entangled state.

Alice performs a local measurement on her subsystem. In general, this is described by a quantum operation, on the system state, of the following kind

$$P(\sigma) = \sum_k (V_k \otimes I_{H_B})^* \, \sigma \, (V_k \otimes I_{H_B}),$$

where V_k are called Kraus matrices which satisfy

$$\sum_k V_k V_k^* = I_{H_A}.$$

The term

$$I_{H_B}$$

from the expression

$$(V_k \otimes I_{H_B})$$

means that Alice's measurement apparatus does not interact with Bob's subsystem.

Supposing the combined system is prepared in state σ and assuming, for purposes of argument, a non-relativistic situation, immediately (with no time delay) after Alice performs her measurement, the relative state of Bob's system is given by the partial trace of the overall state with respect to Alice's system. In symbols, the relative state of Bob's system after Alice's operation is

$$\mathrm{tr}_{H_A}(P(\sigma))$$

where tr_{H_A} is the partial trace mapping with respect to Alice's system.

One can directly calculate this state:

$$\begin{aligned}
\mathrm{tr}_{H_A}(P(\sigma)) &= \mathrm{tr}_{H_A}\left(\sum_k (V_k \otimes I_{H_B})^* \sigma (V_k \otimes I_{H_B})\right) \\
&= \mathrm{tr}_{H_A}\left(\sum_k \sum_i V_k^* T_i V_k \otimes S_i\right) \\
&= \sum_i \sum_k \mathrm{tr}(V_k^* T_i V_k) S_i \\
&= \sum_i \sum_k \mathrm{tr}(T_i V_k V_k^*) S_i \\
&= \sum_i \mathrm{tr}\left(T_i \sum_k V_k V_k^*\right) S_i \\
&= \sum_i \mathrm{tr}(T_i) S_i \\
&= \mathrm{tr}_{H_A}(\sigma).
\end{aligned}$$

From this it is argued that, statistically, Bob cannot tell the difference between what Alice did and a random measurement (or whether she did anything at all).

Some comments

- If the density operator $P(\sigma)$ is allowed to evolve under the influence of non-local interactions between A and B, then in general the calculation in the proof no longer holds, unless suitable commutation relations are assumed.[9]
- The no-communication theorem thus says shared entanglement alone cannot be used to transmit any information. Compare this with the no-teleportation theorem, which states a classical information channel cannot transmit quantum information. (By *transmit*, we mean transmission with full fidelity.) However, quantum teleportation schemes utilize both resources to achieve what is impossible for either alone.
- The no-communication theorem implies the no-cloning theorem, which states that quantum states cannot be (perfectly) copied. That is, cloning is a sufficient condition for the communication of classical information to occur. To see this, suppose that quantum states could be cloned. Assume parts of a maximally entangled Bell state are distributed to Alice and Bob. Alice could send bits to Bob in the following way: If Alice wishes to transmit a "0", she measures the spin of her electron in the **z** direction, collapsing Bob's state to either $|z+\rangle_B$ or $|z-\rangle_B$. To transmit "1", Alice does nothing to her qubit. Bob creates many copies of his electron's state, and measures the spin of each copy in the **z** direction. Bob will know that Alice has transmitted a "0" if all his measurements will produce the same result; otherwise, his measurements will have outcomes $|z+\rangle_B$ or $|z-\rangle_B$ with equal probability. This would allow Alice and Bob to communicate classical bits between each other (possibly across space-like separations, violating causality).
- The version of the no-communication theorem discussed in this article assumes that the quantum system shared by Alice and Bob is a composite system, i.e. that its underlying Hilbert space is a tensor product whose first factor describes the part of the system that Alice can interact with and whose second factor describes the part of the system that Bob can interact with. In quantum field theory, this assumption can be replaced by the assumption that Alice and Bob are spacelike separated.[10] This alternate version of the no-communication theorem shows that faster-than-light communication cannot be achieved using processes which obey the rules of quantum field theory.
- The proof of the no-communication theorem assumes that all measurable properties of Bob's system can be calculated from its reduced density matrix, which is true given the Born rule for calculating the probability of making various measurements. But this equivalence with the Born rule can also essentially be derived in the opposite direction, in that it's possible to show that the Born rule follows from the assumption that space-like separated events cannot violate causality by affecting each other.[11]

See also

- No-broadcast theorem
- No-cloning theorem
- No-deleting theorem
- No-hiding theorem

- No-teleportation theorem

References

1. Peres, A.; Terno, D. (2004). "Quantum Information and Relativity Theory". *Rev. Mod. Phys*. **76** (1): 93–123. arXiv:quant-ph/0212023 (https://arxiv.org/abs/quant-ph/0212023). Bibcode:2004RvMP...76...93P (https://ui.adsabs.harvard.edu/abs/2004RvMP...76...93P). doi:10.1103/RevModPhys.76.93 (https://doi.org/10.1103%2FRevModPhys.76.93). S2CID 7481797 (https://api.semanticscholar.org/CorpusID:7481797). see page 8
2. Quantum Information, Computation and cryptography, Benatti, Fannes, Floreanini, Petritis: pp 210 - theorem HSV and Lemma 1
3. Lajos Diósi, A Short Course in Quantum Information Theory - An Approach From Theoretical Physics 2006 Ch 10. pp 87
4. Shor, Peter W. (1 April 2004). "Equivalence of Additivity Questions in Quantum Information Theory". *Communications in Mathematical Physics*. **246** (3): 453–472. arXiv:quant-ph/0305035 (https://arxiv.org/abs/quant-ph/0305035). Bibcode:2004CMaPh.246..453S (https://ui.adsabs.harvard.edu/abs/2004CMaPh.246..453S). doi:10.1007/s00220-003-0981-7 (https://doi.org/10.1007%2Fs00220-003-0981-7). S2CID 189829228 (https://api.semanticscholar.org/CorpusID:189829228).
5. Hastings, M. B. (April 2009). "Superadditivity of communication capacity using entangled inputs". *Nature Physics*. **5** (4): 255–257. arXiv:0809.3972 (https://arxiv.org/abs/0809.3972). Bibcode:2009NatPh...5..255H (https://ui.adsabs.harvard.edu/abs/2009NatPh...5..255H). doi:10.1038/nphys1224 (https://doi.org/10.1038%2Fnphys1224). S2CID 199687264 (https://api.semanticscholar.org/CorpusID:199687264).
6. Quantum Information, Computation and cryptography, Benatti, Fannes, Floreanini, Petritis: pp 212
7. Hall, Michael J.W. (1987). "Imprecise measurements and non-locality in quantum mechanics". *Physics Letters A*. **125** (2–3). Elsevier BV: 89–91. Bibcode:1987PhLA..125...89H (https://ui.adsabs.harvard.edu/abs/1987PhLA..125...89H). doi:10.1016/0375-9601(87)90127-7 (https://doi.org/10.1016%2F0375-9601%2887%2990127-7). ISSN 0375-9601 (https://search.worldcat.org/issn/0375-9601).
8. Ghirardi, G. C.; Grassi, R; Rimini, A; Weber, T (1988-05-15). "Experiments of the EPR Type Involving CP-Violation Do not Allow Faster-than-Light Communication between Distant Observers". *Europhysics Letters (EPL)*. **6** (2). IOP Publishing: 95–100. Bibcode:1988EL.....6...95G (https://ui.adsabs.harvard.edu/abs/1988EL.....6...95G). doi:10.1209/0295-5075/6/2/001 (https://doi.org/10.1209%2F0295-5075%2F6%2F2%2F001). ISSN 0295-5075 (https://search.worldcat.org/issn/0295-5075). S2CID 250762344 (https://api.semanticscholar.org/CorpusID:250762344).
9. Peacock, K.A.; Hepburn, B. (1999). "Begging the Signaling Question: Quantum Signaling and the Dynamics of Multiparticle Systems". *Proceedings of the Meeting of the Society of Exact Philosophy*. arXiv:quant-ph/9906036 (https://arxiv.org/abs/quant-ph/9906036). Bibcode:1999quant.ph..6036P (https://ui.adsabs.harvard.edu/abs/1999quant.ph..6036P).
10. Eberhard, Phillippe H.; Ross, Ronald R. (1989), "Quantum field theory cannot provide faster than light communication" (http://www.escholarship.org/uc/item/5604n7md), *Foundations of Physics Letters*, **2** (2): 127–149, Bibcode:1989FoPhL...2..127E (https://ui.adsabs.harvard.edu/abs/1989FoPhL...2..127E), doi:10.1007/bf00696109 (https://doi.org/10.1007%2Fbf00696109), S2CID 123217211 (https://api.semanticscholar.org/CorpusID:123217211)
11. Zurek, Wojciech Hubert. "Environment - Assisted Invariance, Causality, and Probabilities in Quantum Physics." https://arxiv.org/abs/quant-ph/0211037

- Florig, Martin; Summers, Stephen J. (1997). "On the statistical independence of algebras of observables". *Journal of Mathematical Physics*. **38** (3). AIP Publishing: 1318–1328.

Bibcode:1997JMP....38.1318F (https://ui.adsabs.harvard.edu/abs/1997JMP....38.1318F). doi:10.1063/1.531812 (https://doi.org/10.1063%2F1.531812). ISSN 0022-2488 (https://search.worldcat.org/issn/0022-2488).

Retrieved from "https://en.wikipedia.org/w/index.php?title=No-communication_theorem&oldid=1229535960"

WIKIPEDIA
The Free Encyclopedia

No-deleting theorem

In physics, the **no-deleting theorem** of quantum information theory is a no-go theorem which states that, in general, given two copies of some arbitrary quantum state, it is impossible to delete one of the copies. It is a time-reversed dual to the no-cloning theorem,[1][2] which states that arbitrary states cannot be copied. It was proved by Arun K. Pati and Samuel L. Braunstein.[3] Intuitively, it is because information is conserved under unitary evolution.[4]

This theorem seems remarkable, because, in many senses, quantum states are fragile; the theorem asserts that, in a particular case, they are also robust.

The no-deleting theorem, together with the no-cloning theorem, underpin the interpretation of quantum mechanics in terms of category theory, and, in particular, as a dagger symmetric monoidal category.[5][6] This formulation, known as categorical quantum mechanics, in turn allows a connection to be made from quantum mechanics to linear logic as the logic of quantum information theory (in exact analogy to classical logic being founded on Cartesian closed categories).

Overview

Suppose that there are two copies of an unknown quantum state. A pertinent question in this context is to ask if it is possible, given two identical copies, to delete one of them using quantum mechanical operations? It turns out that one cannot. The no-deleting theorem is a consequence of linearity of quantum mechanics. Like the no-cloning theorem this has important implications in quantum computing, quantum information theory and quantum mechanics in general.

The process of quantum deleting takes two copies of an arbitrary, unknown quantum state at the input port and outputs a blank state along with the original. Mathematically, this can be described by:

$$U|\psi\rangle_A|\psi\rangle_B|A\rangle_C = |\psi\rangle_A|0\rangle_B|A'\rangle_C$$

where U is a unitary operator, $|\psi\rangle_A$ is the unknown quantum state, $|0\rangle_B$ is the blank state, $|A\rangle_C$ is the initial state of the deleting machine and $|A'\rangle_C$ is the final state of the machine.

It may be noted that classical bits can be copied and deleted, as can qubits in orthogonal states. For example, if we have two identical qubits $|00\rangle$ and $|11\rangle$ then we can transform to $|00\rangle$ and $|10\rangle$. In this case we have deleted the second copy. However, it follows from linearity of quantum theory that there is no U that can perform the deleting operation for any arbitrary state $|\psi\rangle$.

Formal statement

Given three Hilbert spaces for systems A, B, C, such that the Hilbert spaces for systems A, B are identical.

If U is a unitary transformation, and $|A\rangle_C$ is an ancilla state, such that

$$U|\psi\rangle_A|\psi\rangle_B|A\rangle_C = |\psi\rangle_A|0\rangle_B|A_\psi\rangle_C, \quad \forall|\psi\rangle$$

where the final state of the ancilla $|A_\psi\rangle_C$ may depend on $|\psi\rangle$, then U is a swapping operation, in the sense that the map $|\psi\rangle_A \mapsto |A_\psi\rangle_C$ is an isometric embedding.

Proof

The theorem holds for quantum states in a Hilbert space of any dimension. For simplicity, consider the deleting transformation for two identical qubits. If two qubits are in orthogonal states, then deletion requires that

$$\begin{aligned}
|0\rangle_A|0\rangle_B|A\rangle_C &\to |0\rangle_A|0\rangle_B|A_0\rangle_C, \\
|1\rangle_A|1\rangle_B|A\rangle_C &\to |1\rangle_A|0\rangle_B|A_1\rangle_C.
\end{aligned}$$

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the state of an unknown qubit. If we have two copies of an unknown qubit, then by linearity of the deleting transformation we have

$$\begin{aligned}
|\psi\rangle_A|\psi\rangle_B|A\rangle_C &= [\alpha^2|0\rangle_A|0\rangle_B + \beta^2|1\rangle_A|1\rangle_B + \alpha\beta(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)]|A\rangle_C \\
&\to \alpha^2|0\rangle_A|0\rangle_B|A_0\rangle_C + \beta^2|1\rangle_A|0\rangle_B|A_1\rangle_C + \sqrt{2}\alpha\beta|\Phi\rangle_{ABC}.
\end{aligned}$$

In the above expression, the following transformation has been used:

$$1/\sqrt{2}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)|A\rangle_C \to |\Phi\rangle_{ABC}.$$

However, if we are able to delete a copy, then, at the output port of the deleting machine, the combined state should be

$$|\psi\rangle_A|0\rangle_B|A'\rangle_C = (\alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|0\rangle_B)|A'\rangle_C.$$

In general, these states are not identical and hence we can say that the machine fails to delete a copy. If we require that the final output states are same, then we will see that there is only one option:

$$|\Phi\rangle = 1/\sqrt{2}(|0\rangle_A|0\rangle_B|A_1\rangle_C + |1\rangle_A|0\rangle_B|A_0\rangle_C),$$

and

$$|A'\rangle_C = \alpha|A_0\rangle_C + \beta|A_1\rangle_C.$$

Since final state $|A'\rangle$ of the ancilla is normalized for all values of α, β it must be true that $|A_0\rangle_C$ and $|A_1\rangle_C$ are orthogonal. This means that the quantum information is simply in the final state of the ancilla. One can always obtain the unknown state from the final state of the ancilla using local operation on the ancilla Hilbert space. Thus, linearity of quantum theory does not allow an unknown quantum state to be deleted perfectly.

Consequence

- If it were possible to delete an unknown quantum state, then, using two pairs of EPR states, we could send signals faster than light. Thus, violation of the no-deleting theorem is inconsistent with the no-signalling condition.
- The no-cloning and the no-deleting theorems point to the conservation of quantum information.
- Stronger versions of the no-cloning theorem and the no-deleting theorem provide permanence to quantum information. To create a copy one must import the information from some part of the universe and to delete a state one needs to export it to another part of the universe where it will continue to exist.

See also

- No-broadcast theorem
- No-cloning theorem
- No-communication theorem
- No-hiding theorem[7]
- Quantum cloning
- Quantum entanglement
- Quantum information
- Quantum teleportation
- Uncertainty principle
- Landauer's principle

References

1. W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot be Cloned", *Nature* **299** (1982), p802.
2. D. Dieks, "Communication by EPR devices", *Physics Letters A*, vol. **92**(6) (1982), p271.
3. A. K. Pati and S. L. Braunstein, "Impossibility of Deleting an Unknown Quantum State", *Nature* **404** (2000), p164.
4. Horodecki, Michał; Horodecki, Ryszard; Sen(De), Aditi; Sen, Ujjwal (2005-12-01). "Common Origin of No-Cloning and No-Deleting Principles Conservation of Information" (https://doi.org/10.1007/s10701-005-8661-4). *Foundations of Physics*. **35** (12): 2041–2049. arXiv:quant-ph/0407038 (https://arxiv.org/abs/quant-ph/0407038). doi:10.1007/s10701-005-8661-4 (https://doi.org/10.1007%2Fs10701-005-8661-4). ISSN 1572-9516 (https://search.worldcat.org/issn/1572-9516).
5. John Baez, *Physics, Topology, Logic and Computation: A Rosetta Stone (http://math.ucr.edu/home/baez/rosetta.pdf)* (2009)

6. Bob Coecke, *Quantum Picturalism*, (2009) ArXiv 0908.1787 (https://arxiv.org/abs/0908.1787)
7. Quantum no-hiding theorem experimentally confirmed for first time. Mar 07, 2011 by Lisa Zyga (http://phys.org/news/2011-03-quantum-no-hiding-theorem-experimentally.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=No-deleting_theorem&oldid=1225858763"

WIKIPEDIA
The Free Encyclopedia

No-hiding theorem

The **no-hiding theorem**[1] states that if information is lost from a system via decoherence, then it moves to the subspace of the environment and it cannot remain in the correlation between the system and the environment. This is a fundamental consequence of the linearity and unitarity of quantum mechanics. Thus, information is never lost. This has implications in the black hole information paradox and in fact any process that tends to lose information completely. The no-hiding theorem is robust to imperfection in the physical process that seemingly destroys the original information.

This was proved by Samuel L. Braunstein and Arun K. Pati in 2007. In 2011, the no-hiding theorem was experimentally tested[2] using nuclear magnetic resonance devices where a single qubit undergoes complete randomization; i.e., a pure state transforms to a random mixed state. Subsequently, the lost information has been recovered from the ancilla qubits using suitable local unitary transformation only in the environment Hilbert space in accordance with the no-hiding theorem. This experiment for the first time demonstrated the conservation of quantum information.[3]

Formal statement

Let $|\psi\rangle$ be an arbitrary quantum state in some Hilbert space and let there be a physical process that transforms $|\psi\rangle\langle\psi| \to \rho$ with $\rho = \sum_k p_k |k\rangle\langle k|$.
If ρ is independent of the input state $|\psi\rangle$, then in the enlarged Hilbert space the mapping is of the form

$$|\psi\rangle \otimes |A\rangle \to \sum_k \sqrt{p_k}|k\rangle \otimes |A_k(\psi)\rangle = \sum_k \sqrt{p_k}|k\rangle \otimes (|q_k\rangle \otimes |\psi\rangle \oplus 0),$$

where $|A\rangle$ is the initial state of the environment, $|A_k(\psi)\rangle$'s are the orthonormal basis of the environment Hilbert space and $\oplus 0$ denotes the fact that one may augment the unused dimension of the environment Hilbert space by zero vectors.

The proof of the no-hiding theorem is based on the linearity and the unitarity of quantum mechanics. The original information which is missing from the final state simply remains in the subspace of the environmental Hilbert space. Also, note that the original information is not in the correlation between the system and the environment. This is the essence of the no-hiding theorem. One can in principle, recover the lost information from the environment by local unitary transformations acting only on the environment Hilbert space. The no-hiding theorem provides new insights to the nature of quantum information. For example, if classical information is lost from one system it may either move to another system or can be hidden in the correlation between a pair of bit strings. However, quantum information cannot be completely hidden in correlations between a pair of subsystems. Quantum mechanics allows only one way to completely hide an arbitrary quantum state from one of its subsystems. If it is lost from one subsystem, then it moves to other subsystems.

Conservation of quantum information

In physics, conservation laws play important roles. For example, the law of conservation of energy states that the energy of a closed system must remain constant. It can neither increase nor decrease without coming in contact with an external system. If we consider the whole universe as a closed system, the total amount of energy always remains the same. However, the form of energy keeps changing. One may wonder if there is any such law for the conservation of information. In the classical world, information can be copied and deleted perfectly. In the quantum world, however, the conservation of quantum information should mean that information cannot be created nor destroyed. This concept stems from two fundamental theorems of quantum mechanics: the no-cloning theorem and the no-deleting theorem. But the no-hiding theorem is a more general proof of conservation of quantum information which originates from the proof of conservation of wave function in quantum theory. It may be noted that the conservation of entropy holds for a quantum system undergoing unitary time evolution and if entropy represents information in quantum theory, then it is believed then that information should somehow be conserved. For example, one can prove that pure states remain pure states and probabilistic combination of pure states (called as mixed states) remain mixed states under unitary evolution. However, it was never proved that if the probability amplitude disappears from one system, it will reappear in another system. Now, using the no-hiding theorem one can make a precise statement. One may say that as energy keeps changing its form, the wave function keep moving from one Hilbert space to another Hilbert space. Since the wave function contains all the relevant information about a physical system, the conservation of wave function is tantamount to conservation of quantum information.

References

1. Braunstein, Samuel L.; Pati, Arun K. (2007-02-23). "Quantum Information Cannot Be Completely Hidden in Correlations: Implications for the Black-Hole Information Paradox". *Physical Review Letters*. **98** (8): 080502. arXiv:gr-qc/0603046 (https://arxiv.org/abs/gr-qc/0603046). Bibcode:2007PhRvL..98h0502B (https://ui.adsabs.harvard.edu/abs/2007PhRvL..98h0502B). doi:10.1103/physrevlett.98.080502 (https://doi.org/10.1103%2Fphysrevlett.98.080502). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 17359079 (https://pubmed.ncbi.nlm.nih.gov/17359079). S2CID 9897809 (https://api.semanticscholar.org/CorpusID:9897809).
2. Samal, Jharana Rani; Pati, Arun K.; Kumar, Anil (2011-02-22). "Experimental Test of the Quantum No-Hiding Theorem". *Physical Review Letters*. **106** (8): 080401. arXiv:1004.5073 (https://arxiv.org/abs/1004.5073). Bibcode:2011PhRvL.106h0401S (https://ui.adsabs.harvard.edu/abs/2011PhRvL.106h0401S). doi:10.1103/physrevlett.106.080401 (https://doi.org/10.1103%2Fphysrevlett.106.080401). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 21405552 (https://pubmed.ncbi.nlm.nih.gov/21405552). S2CID 43280895 (https://api.semanticscholar.org/CorpusID:43280895).
3. Zyga, Lisa (2011-03-07). "Quantum no-hiding theorem experimentally confirmed for first time" (https://phys.org/news/2011-03-quantum-no-hiding-theorem-experimentally.html). *Phys.org*. Retrieved 2019-08-18.

Retrieved from "https://en.wikipedia.org/w/index.php?title=No-hiding_theorem&oldid=1239095750"

WIKIPEDIA
The Free Encyclopedia

No-teleportation theorem

In quantum information theory, the **no-teleportation theorem** states that an arbitrary quantum state cannot be converted into a sequence of classical bits (or even an infinite number of such bits); nor can such bits be used to reconstruct the original state, thus "teleporting" it by merely moving classical bits around. Put another way, it states that the unit of quantum information, the qubit, cannot be exactly, precisely converted into classical information bits. This should not be confused with quantum teleportation, which does allow a quantum state to be destroyed in one location, and an exact replica to be created at a different location.

In crude terms, the no-teleportation theorem stems from the Heisenberg uncertainty principle and the EPR paradox: although a qubit $|\psi\rangle$ can be imagined to be a specific direction on the Bloch sphere, that direction cannot be measured precisely, for the general case $|\psi\rangle$; if it could, the results of that measurement would be describable with words, i.e. classical information.

The no-teleportation theorem is implied by the no-cloning theorem: if it were possible to convert a qubit into classical bits, then a qubit would be easy to copy (since classical bits are trivially copyable).

Formulation

The term *quantum information* refers to information stored in the state of a quantum system. Two quantum states ρ_1 and ρ_2 are identical if the measurement results of any physical observable have the same expectation value for ρ_1 and ρ_2. Thus measurement can be viewed as an information channel with quantum input and classical output, that is, performing measurement on a quantum system transforms quantum information into classical information. On the other hand, preparing a quantum state takes classical information to quantum information.

In general, a quantum state is described by a density matrix. Suppose one has a quantum system in some mixed state ρ. Prepare an ensemble, of the same system, as follows:

1. Perform a measurement on ρ.
2. According to the measurement outcome, prepare a system in some pre-specified state.

The no-teleportation theorem states that the result will be different from ρ, irrespective of how the preparation procedure is related to measurement outcome. A quantum state cannot be determined via a single measurement. In other words, if a quantum channel measurement is followed by preparation, it cannot be the identity channel. Once converted to classical information, quantum information cannot be recovered.

In contrast, perfect transmission is possible if one wishes to convert classical information to quantum information then back to classical information. For classical bits, this can be done by encoding them in orthogonal quantum states, which can always be distinguished.

See also

Among other no-go theorems in quantum information are:

- No-communication theorem. Entangled states cannot be used to transmit classical information.
- No-cloning theorem. Quantum states cannot be copied.
- No-broadcast theorem. A generalization of the no cloning theorem, to the case of mixed states.
- No-deleting theorem. A result dual to the no-cloning theorem: copies cannot be deleted.

With the aid of shared entanglement, quantum states can be teleported, see

- Quantum teleportation

References

- Jozef Gruska, Iroshi Imai, "Power, Puzzles and Properties of Entanglement" (2001) pp 25–68, appearing in *Machines, Computations, and Universality: Third International Conference.* edited by Maurice Margenstern, Yurii Rogozhin. (see p 41 (https://books.google.com/books?id=iahtCQAAQBAJ&pg=PA41&lpg=PA41&dq=no+teleportation+theorem))
- Anirban Pathak, *Elements of Quantum Computation and Quantum Communication* (2013) CRC Press. (see p. 128 (https://books.google.com/books?id=cEPSBQAAQBAJ&pg=PA128&lpg=PA128&dq=no+teleportation+theorem))

Retrieved from "https://en.wikipedia.org/w/index.php?title=No-teleportation_theorem&oldid=1132280110"

WIKIPEDIA
The Free Encyclopedia

Quantum speed limit

In quantum mechanics, a **quantum speed limit** (**QSL**) is a limitation on the minimum time for a quantum system to evolve between two distinguishable (orthogonal) states.[1] QSL theorems are closely related to time-energy uncertainty relations. In 1945, Leonid Mandelstam and Igor Tamm derived a time-energy uncertainty relation that bounds the speed of evolution in terms of the energy dispersion.[2] Over half a century later, Norman Margolus and Lev Levitin showed that the speed of evolution cannot exceed the mean energy,[3] a result known as the Margolus–Levitin theorem. Realistic physical systems in contact with an environment are known as open quantum systems and their evolution is also subject to QSL.[4][5] Quite remarkably it was shown that environmental effects, such as non-Markovian dynamics can speed up quantum processes,[6] which was verified in a cavity QED experiment.[7]

QSL have been used to explore the limits of computation[8][9] and complexity. In 2017, QSLs were studied in a quantum oscillator at high temperature.[10] In 2018, it was shown that QSL are not restricted to the quantum domain and that similar bounds hold in classical systems.[11][12] In 2021, both the Mandelstam-Tamm and the Margolus–Levitin QSL bounds were concurrently tested in a single experiment[13] which indicated there are "two different regimes: one where the Mandelstam-Tamm limit constrains the evolution at all times, and a second where a crossover to the Margolus-Levitin limit occurs at longer times."

Preliminary definitions

The speed limit theorems can be stated for pure states, and for mixed states; they take a simpler form for pure states. An arbitrary pure state can be written as a linear combination of energy eigenstates:

$$|\psi\rangle = \sum_n c_n |E_n\rangle.$$

The task is to provide a lower bound for the time interval $t_\perp$ required for the initial state $|\psi\rangle$ to evolve into a state orthogonal to $|\psi\rangle$. The time evolution of a pure state is given by the Schrödinger equation:

$$|\psi_t\rangle = \sum_n c_n e^{itE_n/\hbar} |E_n\rangle.$$

Orthogonality is obtained when

$$\langle \psi_0 | \psi_t \rangle = 0$$

and the minimum time interval $t = t_\perp$ required to achieve this condition is called the orthogonalization interval[2] or orthogonalization time.[14]

Mandelstam–Tamm limit

For pure states, the Mandelstam–Tamm theorem states that the minimum time $t_\perp$ required for a state to evolve into an orthogonal state is bounded below:

$$t_\perp \geq \frac{\pi\hbar}{2\,\delta E} = \frac{h}{4\,\delta E},$$

where

$$(\delta E)^2 = \langle\psi|H^2|\psi\rangle - (\langle\psi|H|\psi\rangle)^2 = \frac{1}{2}\sum_{n,m}|c_n|^2|c_m|^2(E_n - E_m)^2,$$

is the variance of the system's energy and H is the Hamiltonian operator. The quantum evolution is independent of the particular Hamiltonian used to transport the quantum system along a given curve in the projective Hilbert space; the distance along this curve is measured by the Fubini–Study metric.[15] This is sometimes called the quantum angle, as it can be understood as the arccos of the inner product of the initial and final states.

For mixed states

The Mandelstam–Tamm limit can also be stated for mixed states and for time-varying Hamiltonians. In this case, the Bures metric must be employed in place of the Fubini–Study metric. A mixed state can be understood as a sum over pure states, weighted by classical probabilities; likewise, the Bures metric is a weighted sum of the Fubini–Study metric. For a time-varying Hamiltonian H_t and time-varying density matrix ρ_t, the variance of the energy is given by

$$\sigma_H^2(t) = |\mathrm{tr}(\rho_t H_t^2)| - |\mathrm{tr}(\rho_t H_t)|^2$$

The Mandelstam–Tamm limit then takes the form

$$\int_0^\tau \sigma_H(t)dt \geq \hbar D_B(\rho_0, \rho_\tau),$$

where D_B is the Bures distance between the starting and ending states. The Bures distance is geodesic, giving the shortest possible distance of any continuous curve connecting two points, with $\sigma_H(t)$ understood as an infinitessimal path length along a curve parametrized by t. Equivalently, the time τ taken to evolve from ρ to ρ' is bounded as

$$\tau \geq \frac{\hbar}{\overline{\sigma}_H} D_B(\rho, \rho')$$

where

$$\overline{\sigma}_H = \frac{1}{\tau}\int_0^\tau \sigma_H(t)dt$$

is the time-averaged uncertainty in energy. For a pure state evolving under a time-varying Hamiltonian, the time τ taken to evolve from one pure state to another pure state orthogonal to it is bounded as[16]

$$\tau \geq \frac{\hbar}{\overline{\sigma}_H} \frac{\pi}{2}$$

This follows, as for a pure state, one has the density matrix $\rho_t = |\psi_t\rangle\langle\psi_t|$. The quantum angle (Fubini–Study distance) is then $D_B(\rho_0, \rho_t) = \arccos |\langle\psi_0|\psi_t\rangle|$ and so one concludes $D_B = \arccos 0 = \pi/2$ when the initial and final states are orthogonal.

Margolus–Levitin limit

For the case of a pure state, Margolus and Levitin[3] obtain a different limit, that

$$\tau_\perp \geq \frac{h}{4\langle E\rangle},$$

where $\langle E\rangle$ is the average energy,

$$\langle E\rangle = E_{\mathrm{avg}} = \langle\psi|H|\psi\rangle = \sum_n |c_n|^2 E_n.$$

This form applies when the Hamiltonian is not time-dependent, and the ground-state energy is defined to be zero.

For time-varying states

The Margolus–Levitin theorem can also be generalized to the case where the Hamiltonian varies with time, and the system is described by a mixed state.[16] In this form, it is given by

$$\int_0^\tau |\mathrm{tr}(\rho_t H_t)| dt \geq \hbar D_B(\rho_0, \rho_\tau)$$

with the ground-state defined so that it has energy zero at all times.

This provides a result for time varying states. Although it also provides a bound for mixed states, the bound (for mixed states) can be so loose as to be uninformative.[17] The Margolus–Levitin theorem has not yet been established in time-dependent quantum systems, whose Hamiltonians H_t are driven by arbitrary time-dependent parameters, except for the adiabatic case.[18]

Levitin–Toffoli limit

A 2009 result by Lev B. Levitin and Tommaso Toffoli states that the precise bound for the Mandelstam–Tamm theorem is attained only for a qubit state.[14] This is a two-level state in an equal superposition

$$|\psi_q\rangle = \frac{1}{\sqrt{2}} \left(|E_0\rangle + e^{i\varphi} |E_1\rangle\right)$$

for energy eigenstates $E_0 = 0$ and $E_1 = \pm\pi\hbar/\Delta t$. The states $|E_0\rangle$ and $|E_1\rangle$ are unique up to degeneracy of the energy level E_1 and an arbitrary phase factor φ. This result is sharp, in that this state also satisfies the Margolus–Levitin bound, in that $E_{\mathrm{avg}} = \delta E$ and so $t_\perp = \hbar\pi/2E_{\mathrm{avg}} = \hbar\pi/2\delta E$. This result establishes that the combined limits are strict:

$$t_\perp \geq \max\left(\frac{\pi\hbar}{2\,\delta E}\ ,\ \frac{\pi\hbar}{2\,E_{\mathrm{avg}}}\right)$$

Levitin and Toffoli also provide a bound for the average energy in terms of the maximum. For any pure state $|\psi\rangle$, the average energy is bounded as

$$\frac{E_{\max}}{4} \leq E_{\mathrm{avg}} \leq \frac{E_{\max}}{2}$$

where $E_{\max}$ is the maximum energy eigenvalue appearing in $|\psi\rangle$. (This is the quarter-pinched sphere theorem in disguise, transported to complex projective space.) Thus, one has the bound

$$\frac{\pi\hbar}{E_{\max}} \leq t_\perp \leq \frac{2\pi\hbar}{E_{\max}}$$

The strict lower bound $E_{\max} t_\perp = \pi\hbar$ is again attained for the qubit state $|\psi_q\rangle$ with $E_{\max} = E_1$.

Bremermann's limit

The quantum speed limit bounds establish an upper bound at which computation can be performed. Computational machinery is constructed out of physical matter that follows quantum mechanics, and each operation, if it is to be unambiguous, must be a transition of the system from one state to an orthogonal state. Suppose the computing machinery is a physical system evolving under Hamiltonian that does not change with time. Then, according to the Margolus–Levitin theorem, the number of operations per unit time per unit energy is bounded above by

$$\frac{2}{\hbar\pi} = 6 \times 10^{33}\mathrm{s}^{-1} \cdot \mathrm{J}^{-1}$$

This establishes a strict upper limit on the number of calculations that can be performed by physical matter. The processing rate of *all* forms of computation cannot be higher than about 6×10^{33} operations per second per joule of energy. This is including "classical" computers, since even classical computers are still made of matter that follows quantum mechanics.[19][20]

This bound is not merely a fanciful limit: it has practical ramifications for quantum-resistant cryptography. Imagining a computer operating at this limit, a brute-force search to break a 128-bit encryption key requires only modest resources. Brute-forcing a 256-bit key requires planetary-scale computers, while a brute-force search of 512-bit keys is effectively unattainable within the lifetime of the universe, even if galactic-sized computers were applied to the problem.

The Bekenstein bound limits the amount of information that can be stored within a volume of space. The maximal rate of change of information within that volume of space is given by the quantum speed limit. This product of limits is sometimes called the **Bremermann–Bekenstein limit**; it is saturated by

Hawking radiation.[1] That is, Hawking radiation is emitted at the maximal allowed rate set by these bounds.

References

1. Deffner, S.; Campbell, S. (10 October 2017). "Quantum speed limits: from Heisenberg's uncertainty principle to optimal quantum control". *J. Phys. A: Math. Theor.* **50** (45): 453001. arXiv:1705.08023 (https://arxiv.org/abs/1705.08023). Bibcode:2017JPhA...50S3001D (https://ui.adsabs.harvard.edu/abs/2017JPhA...50S3001D). doi:10.1088/1751-8121/aa86c6 (https://doi.org/10.1088%2F1751-8121%2Faa86c6). S2CID 3477317 (https://api.semanticscholar.org/CorpusID:3477317).
2. Mandelshtam, L. I.; Tamm, I. E. (1945). "The uncertainty relation between energy and time in nonrelativistic quantum mechanics". *J. Phys. (USSR)*. **9**: 249–254. Reprinted as Mandelstam, L.; Tamm, Ig. (1991). "The Uncertainty Relation Between Energy and Time in Non-relativistic Quantum Mechanics". In Bolotovskii, Boris M.; Frenkel, Victor Ya.; Peierls, Rudolf (eds.). *Selected Papers* (http://link.springer.com/10.1007/978-3-642-74626-0_8). Berlin, Heidelberg: Springer. pp. 115–123. doi:10.1007/978-3-642-74626-0_8 (https://doi.org/10.1007%2F978-3-642-74626-0_8). ISBN 978-3-642-74628-4. Retrieved 2024-04-06.
3. Margolus, Norman; Levitin, Lev B. (September 1998). "The maximum speed of dynamical evolution". *Physica D: Nonlinear Phenomena*. **120** (1–2): 188–195. arXiv:quant-ph/9710043 (https://arxiv.org/abs/quant-ph/9710043). Bibcode:1998PhyD..120..188M (https://ui.adsabs.harvard.edu/abs/1998PhyD..120..188M). doi:10.1016/S0167-2789(98)00054-2 (https://doi.org/10.1016%2FS0167-2789%2898%2900054-2). S2CID 468290 (https://api.semanticscholar.org/CorpusID:468290).
4. Taddei, M. M.; Escher, B. M.; Davidovich, L.; de Matos Filho, R. L. (30 January 2013). "Quantum Speed Limit for Physical Processes". *Physical Review Letters*. **110** (5): 050402. arXiv:1209.0362 (https://arxiv.org/abs/1209.0362). Bibcode:2013PhRvL.110e0402T (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110e0402T). doi:10.1103/PhysRevLett.110.050402 (https://doi.org/10.1103%2FPhysRevLett.110.050402). PMID 23414007 (https://pubmed.ncbi.nlm.nih.gov/23414007). S2CID 38373815 (https://api.semanticscholar.org/CorpusID:38373815).
5. del Campo, A.; Egusquiza, I. L.; Plenio, M. B.; Huelga, S. F. (30 January 2013). "Quantum Speed Limits in Open System Dynamics". *Physical Review Letters*. **110** (5): 050403. arXiv:1209.1737 (https://arxiv.org/abs/1209.1737). Bibcode:2013PhRvL.110e0403D (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110e0403D). doi:10.1103/PhysRevLett.110.050403 (https://doi.org/10.1103%2FPhysRevLett.110.050403). PMID 23414008 (https://pubmed.ncbi.nlm.nih.gov/23414008). S2CID 8362503 (https://api.semanticscholar.org/CorpusID:8362503).
6. Deffner, S.; Lutz, E. (3 July 2013). "Quantum speed limit for non-Markovian dynamics". *Physical Review Letters*. **111** (1): 010402. arXiv:1302.5069 (https://arxiv.org/abs/1302.5069). Bibcode:2013PhRvL.111a0402D (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111a0402D). doi:10.1103/PhysRevLett.111.010402 (https://doi.org/10.1103%2FPhysRevLett.111.010402). PMID 23862985 (https://pubmed.ncbi.nlm.nih.gov/23862985). S2CID 36711861 (https://api.semanticscholar.org/CorpusID:36711861).
7. Cimmarusti, A. D.; Yan, Z.; Patterson, B. D.; Corcos, L. P.; Orozco, L. A.; Deffner, S. (11 June 2015). "Environment-Assisted Speed-up of the Field Evolution in Cavity Quantum Electrodynamics". *Physical Review Letters*. **114** (23): 233602. arXiv:1503.02591 (https://arxiv.org/abs/1503.02591). Bibcode:2015PhRvL.114w3602C (https://ui.adsabs.harvard.edu/abs/2015PhRvL.114w3602C). doi:10.1103/PhysRevLett.114.233602 (https://doi.org/10.1103%2FPhysRevLett.114.233602). PMID 26196802 (https://pubmed.ncbi.nlm.nih.gov/26196802). S2CID 14904633 (https://api.semanticscholar.org/CorpusID:14904633).

8. Lloyd, Seth (31 August 2000). "Ultimate physical limits to computation". *Nature*. **406** (6799): 1047–1054. arXiv:quant-ph/9908043 (https://arxiv.org/abs/quant-ph/9908043). Bibcode:2000Natur.406.1047L (https://ui.adsabs.harvard.edu/abs/2000Natur.406.1047L). doi:10.1038/35023282 (https://doi.org/10.1038%2F35023282). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 10984064 (https://pubmed.ncbi.nlm.nih.gov/10984064). S2CID 75923 (https://api.semanticscholar.org/CorpusID:75923).
9. Lloyd, Seth (24 May 2002). "Computational Capacity of the Universe". *Physical Review Letters*. **88** (23): 237901. arXiv:quant-ph/0110141 (https://arxiv.org/abs/quant-ph/0110141). Bibcode:2002PhRvL..88w7901L (https://ui.adsabs.harvard.edu/abs/2002PhRvL..88w7901L). doi:10.1103/PhysRevLett.88.237901 (https://doi.org/10.1103%2FPhysRevLett.88.237901). PMID 12059399 (https://pubmed.ncbi.nlm.nih.gov/12059399). S2CID 6341263 (https://api.semanticscholar.org/CorpusID:6341263).
10. Deffner, S. (20 October 2017). "Geometric quantum speed limits: a case for Wigner phase space" (https://doi.org/10.1088%2F1367-2630%2Faa83dc). *New Journal of Physics*. **19** (10): 103018. arXiv:1704.03357 (https://arxiv.org/abs/1704.03357). Bibcode:2017NJPh...19j3018D (https://ui.adsabs.harvard.edu/abs/2017NJPh...19j3018D). doi:10.1088/1367-2630/aa83dc (https://doi.org/10.1088%2F1367-2630%2Faa83dc). hdl:11603/19409 (https://hdl.handle.net/11603%2F19409).
11. Shanahan, B.; Chenu, A.; Margolus, N.; del Campo, A. (12 February 2018). "Quantum Speed Limits across the Quantum-to-Classical Transition" (https://doi.org/10.1103%2FPhysRevLett.120.070401). *Physical Review Letters*. **120** (7): 070401. arXiv:1710.07335 (https://arxiv.org/abs/1710.07335). Bibcode:2018PhRvL.120g0401S (https://ui.adsabs.harvard.edu/abs/2018PhRvL.120g0401S). doi:10.1103/PhysRevLett.120.070401 (https://doi.org/10.1103%2FPhysRevLett.120.070401). PMID 29542956 (https://pubmed.ncbi.nlm.nih.gov/29542956).
12. Okuyama, Manaka; Ohzeki, Masayuki (12 February 2018). "Quantum Speed Limit is Not Quantum". *Physical Review Letters*. **120** (7): 070402. arXiv:1710.03498 (https://arxiv.org/abs/1710.03498). Bibcode:2018PhRvL.120g0402O (https://ui.adsabs.harvard.edu/abs/2018PhRvL.120g0402O). doi:10.1103/PhysRevLett.120.070402 (https://doi.org/10.1103%2FPhysRevLett.120.070402). PMID 29542975 (https://pubmed.ncbi.nlm.nih.gov/29542975). S2CID 4027745 (https://api.semanticscholar.org/CorpusID:4027745).
13. Ness, Gal; Lam, Manolo R.; Alt, Wolfgang; Meschede, Dieter; Sagi, Yoav; Alberti, Andrea (22 December 2021). "Observing crossover between quantum speed limits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8694601). *Science Advances*. **7** (52): eabj9119. doi:10.1126/sciadv.abj9119 (https://doi.org/10.1126%2Fsciadv.abj9119). PMC 8694601 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8694601). PMID 34936463 (https://pubmed.ncbi.nlm.nih.gov/34936463).
14. Lev B. Levitin; Tommaso Toffoli (2009), "Fundamental Limit on the Rate of Quantum Dynamics: The Unified Bound Is Tight" (https://link.aps.org/doi/10.1103/PhysRevLett.103.160502), *Physical Review Letters*, **103** (16): 160502, arXiv:0905.3417 (https://arxiv.org/abs/0905.3417), Bibcode:2009PhRvL.103p0502L (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103p0502L), doi:10.1103/PhysRevLett.103.160502 (https://doi.org/10.1103%2FPhysRevLett.103.160502), ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007), PMID 19905679 (https://pubmed.ncbi.nlm.nih.gov/19905679), S2CID 36320152 (https://api.semanticscholar.org/CorpusID:36320152)
15. Aharonov, Yakir; Anandan, Jeeva (1990). "Geometry of quantum evolution". *Physical Review Letters*. **65** (14): 1697–1700. Bibcode:1990PhRvL..65.1697A (https://ui.adsabs.harvard.edu/abs/1990PhRvL..65.1697A). doi:10.1103/PhysRevLett.65.1697 (https://doi.org/10.1103%2FPhysRevLett.65.1697). PMID 10042340 (https://pubmed.ncbi.nlm.nih.gov/10042340).

16. Deffner, Sebastian; Lutz, Eric (2013-08-23). "Energy–time uncertainty relation for driven quantum systems" (https://iopscience.iop.org/article/10.1088/1751-8113/46/33/335302). *Journal of Physics A: Mathematical and Theoretical*. **46** (33): 335302. arXiv:1104.5104 (https://arxiv.org/abs/1104.5104). Bibcode:2013JPhA...46G5302D (https://ui.adsabs.harvard.edu/abs/2013JPhA...46G5302D). doi:10.1088/1751-8113/46/33/335302 (https://doi.org/10.1088%2F1751-8113%2F46%2F33%2F335302). hdl:11603/19394 (https://hdl.handle.net/11603%2F19394). ISSN 1751-8113 (https://search.worldcat.org/issn/1751-8113). S2CID 119313370 (https://api.semanticscholar.org/CorpusID:119313370).
17. Marvian, Iman; Spekkens, Robert W.; Zanardi, Paolo (2016-05-24). "Quantum speed limits, coherence, and asymmetry" (https://link.aps.org/doi/10.1103/PhysRevA.93.052331). *Physical Review A*. **93** (5): 052331. arXiv:1510.06474 (https://arxiv.org/abs/1510.06474). Bibcode:2016PhRvA..93e2331M (https://ui.adsabs.harvard.edu/abs/2016PhRvA..93e2331M). doi:10.1103/PhysRevA.93.052331 (https://doi.org/10.1103%2FPhysRevA.93.052331). ISSN 2469-9926 (https://search.worldcat.org/issn/2469-9926).
18. Okuyama, Manaka; Ohzeki, Masayuki (2018). "Comment on 'Energy-time uncertainty relation for driven quantum systems' " (https://iopscience.iop.org/article/10.1088/1751-8121/aacb90). *Journal of Physics A: Mathematical and Theoretical*. **51** (31): 318001. arXiv:1802.00995 (https://arxiv.org/abs/1802.00995). Bibcode:2018JPhA...51E8001O (https://ui.adsabs.harvard.edu/abs/2018JPhA...51E8001O). doi:10.1088/1751-8121/aacb90 (https://doi.org/10.1088%2F1751-8121%2Faacb90). ISSN 1751-8113 (https://search.worldcat.org/issn/1751-8113).
19. Bremermann, H.J. (1962) *Optimization through evolution and recombination* (http://holtz.org/Library/Natural%20Science/Physics/Optimization%20Through%20Evolution%20and%20Recombination%20-%20Bremermann%201962.htm) In: Self-Organizing systems 1962, edited M.C. Yovits et al., Spartan Books, Washington, D.C. pp. 93–106.
20. Bremermann, H.J. (1965) Quantum noise and information (http://projecteuclid.org/euclid.bsmsp/1200513783). 5th Berkeley Symposium on Mathematical Statistics and Probability; Univ. of California Press, Berkeley, California.

Further reading

- Jordan, Stephen P. (2017). "Fast quantum computation at arbitrarily low energy". *Physical Review A*. **95** (3): 032305. arXiv:1701.01175 (https://arxiv.org/abs/1701.01175). Bibcode:2017PhRvA..95c2305J (https://ui.adsabs.harvard.edu/abs/2017PhRvA..95c2305J). doi:10.1103/PhysRevA.95.032305 (https://doi.org/10.1103%2FPhysRevA.95.032305). S2CID 118953874 (https://api.semanticscholar.org/CorpusID:118953874).
- Sinitsyn, Nikolai A. (2018). "Is there a quantum limit on speed of computation?". *Physics Letters A*. **382** (7): 477–481. arXiv:1701.05550 (https://arxiv.org/abs/1701.05550). Bibcode:2018PhLA..382..477S (https://ui.adsabs.harvard.edu/abs/2018PhLA..382..477S). doi:10.1016/j.physleta.2017.12.042 (https://doi.org/10.1016%2Fj.physleta.2017.12.042). S2CID 55887738 (https://api.semanticscholar.org/CorpusID:55887738).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_speed_limit&oldid=1226901320"

WIKIPEDIA
The Free Encyclopedia

Threshold theorem

In quantum computing, the **threshold theorem** (or **quantum fault-tolerance theorem**) states that a quantum computer with a physical error rate below a certain threshold can, through application of quantum error correction schemes, suppress the logical error rate to arbitrarily low levels. This shows that quantum computers can be made fault-tolerant, as an analogue to von Neumann's threshold theorem for classical computation.[1] This result was proven (for various error models) by the groups of Dorit Aharanov and Michael Ben-Or;[2] Emanuel Knill, Raymond Laflamme, and Wojciech Zurek;[3] and Alexei Kitaev[4] independently.[3] These results built on a paper of Peter Shor,[5] which proved a weaker version of the threshold theorem.

Explanation

The key question that the threshold theorem resolves is whether quantum computers in practice could perform long computations without succumbing to noise. Since a quantum computer will not be able to perform gate operations perfectly, some small constant error is inevitable; hypothetically, this could mean that quantum computers with imperfect gates can only apply a constant number of gates before the computation is destroyed by noise.

Surprisingly, the quantum threshold theorem shows that if the error to perform each gate is a small enough constant, one can perform arbitrarily long quantum computations to arbitrarily good precision, with only some small added overhead in the number of gates. The formal statement of the threshold theorem depends on the types of error correction codes and error model being considered. *Quantum Computation and Quantum Information*, by Michael Nielsen and Isaac Chuang, gives the general framework for such a theorem:

Threshold theorem for quantum computation[6]:481**:** A quantum circuit on n qubits and containing $p(n)$ gates may be simulated with probability of error at most ε using

$$O(\log^c(p(n)/\varepsilon)p(n))$$

gates (for some constant c) on hardware whose components fail with probability at most p, provided p is below some constant *threshold*, $p < p_{\text{th}}$, and given reasonable assumptions about the noise in the underlying hardware.

Threshold theorems for classical computation have the same form as above, except for classical circuits instead of quantum. The proof strategy for quantum computation is similar to that of classical computation: for any particular error model (such as having each gate fail with independent probability p), use error correcting codes to build better gates out of existing gates. Though these "better gates" are larger, and so are more prone to errors within them, their error-correction properties mean that they have a lower chance of failing than the original gate (provided p is a small-enough constant). Then, one can use these better gates to recursively create even better gates, until one has gates with the desired failure probability, which can be used for the desired quantum circuit. According to quantum information theorist Scott Aaronson:

> "The entire content of the Threshold Theorem is that you're correcting errors faster than they're created. That's the whole point, and the whole non-trivial thing that the theorem shows. That's the problem it solves."[7]

Threshold value in practice

Current estimates put the threshold for the surface code on the order of 1%,[8] though estimates range widely and are difficult to calculate due to the exponential difficulty of simulating large quantum systems.[a] At a 0.1% probability of a depolarizing error, the surface code would require approximately 1,000-10,000 physical qubits per logical data qubit,[9] though more pathological error types could change this figure drastically.

See also

- Quantum error correction schemes
- Physical and logical qubits
- Fault tolerance

Notes

a. It is widely believed that it is exponentially difficult for classical computers to simulate quantum systems. This problem is known as the quantum many body problem. However, quantum computers can simulate many (though not all) Hamiltonians in polynomial time with bounded errors, which is one of the main appeals of quantum computing. This is applicable to chemical simulations, drug discovery, energy production, climate modeling and fertilizer production (e.g. FeMoco) as well. Because of this, quantum computers may be better than classical computers at aiding design of further quantum computers.

References

1. Neumann, J. von (1956-12-31), "Probabilistic Logics and the Synthesis of Reliable Organisms From Unreliable Components" (https://dx.doi.org/10.1515/9781400882618-003), *Automata Studies. (AM-34)*, Princeton: Princeton University Press, pp. 43–98, doi:10.1515/9781400882618-003 (https://doi.org/10.1515%2F9781400882618-003), ISBN 978-1-4008-8261-8, retrieved 2020-10-10
2. Aharonov, Dorit; Ben-Or, Michael (2008-01-01). "Fault-Tolerant Quantum Computation with Constant Error Rate" (https://epubs.siam.org/doi/10.1137/S0097539799359385). *SIAM Journal on Computing*. **38** (4): 1207–1282. arXiv:quant-ph/9906129 (https://arxiv.org/abs/quant-ph/9906129). doi:10.1137/S0097539799359385 (https://doi.org/10.1137%2FS0097539799359385). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397). S2CID 8969800 (https://api.semanticscholar.org/CorpusID:8969800).
3. Knill, E. (1998-01-16). "Resilient Quantum Computation" (https://www.science.org/doi/10.1126/science.279.5349.342). *Science*. **279** (5349): 342–345. arXiv:quant-ph/9702058 (https://arxiv.org/abs/quant-ph/9702058). Bibcode:1998Sci...279..342K (https://ui.adsabs.harvard.ed

u/abs/1998Sci...279..342K). doi:10.1126/science.279.5349.342 (https://doi.org/10.1126%2Fscience.279.5349.342).
4. Kitaev, A. Yu. (2003-01-01). "Fault-tolerant quantum computation by anyons" (http://www.sciencedirect.com/science/article/pii/S0003491602000180). *Annals of Physics*. **303** (1): 2–30. arXiv:quant-ph/9707021 (https://arxiv.org/abs/quant-ph/9707021). Bibcode:2003AnPhy.303....2K (https://ui.adsabs.harvard.edu/abs/2003AnPhy.303....2K). doi:10.1016/S0003-4916(02)00018-0 (https://doi.org/10.1016%2FS0003-4916%2802%2900018-0). ISSN 0003-4916 (https://search.worldcat.org/issn/0003-4916). S2CID 119087885 (https://api.semanticscholar.org/CorpusID:119087885).
5. Shor, P.W. (1996). "Fault-tolerant quantum computation" (https://ieeexplore.ieee.org/document/548464). *Proceedings of 37th Conference on Foundations of Computer Science*. Burlington, VT, USA: IEEE Comput. Soc. Press. pp. 56–65. doi:10.1109/SFCS.1996.548464 (https://doi.org/10.1109%2FSFCS.1996.548464). ISBN 978-0-8186-7594-2. S2CID 7508572 (https://api.semanticscholar.org/CorpusID:7508572).
6. Nielsen, Michael A.; Chuang, Isaac L. (June 2012). *Quantum Computation and Quantum Information* (10th anniversary ed.). Cambridge: Cambridge University Press. ISBN 9780511992773. OCLC 700706156 (https://search.worldcat.org/oclc/700706156).
7. Aaronson, Scott; Granade, Chris (Fall 2006). "Lecture 14: Skepticism of Quantum Computing" (https://www.scottaaronson.com/democritus/lec14.html). *PHYS771: Quantum Computing Since Democritus*. Shtetl Optimized. Retrieved 2018-12-27.
8. Fowler, Austin G.; Stephens, Ashley M.; Groszkowski, Peter (2009-11-11). "High-threshold universal quantum computation on the surface code". *Physical Review A*. **80** (5): 052312. arXiv:0803.0272 (https://arxiv.org/abs/0803.0272). Bibcode:2009PhRvA..80e2312F (https://ui.adsabs.harvard.edu/abs/2009PhRvA..80e2312F). doi:10.1103/physreva.80.052312 (https://doi.org/10.1103%2Fphysreva.80.052312). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 119228385 (https://api.semanticscholar.org/CorpusID:119228385).
9. Campbell, Earl T.; Terhal, Barbara M.; Vuillot, Christophe (2017-09-13). "Roads towards fault-tolerant universal quantum computation". *Nature*. **549** (7671): 172–179. arXiv:1612.07330 (https://arxiv.org/abs/1612.07330). Bibcode:2017Natur.549..172C (https://ui.adsabs.harvard.edu/abs/2017Natur.549..172C). doi:10.1038/nature23460 (https://doi.org/10.1038%2Fnature23460). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 28905902 (https://pubmed.ncbi.nlm.nih.gov/28905902). S2CID 4446310 (https://api.semanticscholar.org/CorpusID:4446310).

External links

- Gil Kalai. "Perpetual Motion of The 21st Century?" (http://rjlipton.wordpress.com/2012/01/30/perpetual-motion-of-the-21st-century/).
- Scott Aaronson. "PHYS771 Lecture 14: Skepticism of Quantum Computing" (http://www.scottaaronson.com/democritus/lec14.html): *«The entire content of the Threshold Theorem is that you're correcting errors faster than they're created. That's the whole point, and the whole non-trivial thing that the theorem shows. That's the problem it solves.»*

Retrieved from "https://en.wikipedia.org/w/index.php?title=Threshold_theorem&oldid=1222256839"

WIKIPEDIA
The Free Encyclopedia

Solovay–Kitaev theorem

In quantum information and computation, the **Solovay–Kitaev theorem** says that if a set of single-qubit quantum gates generates a dense subgroup of SU(2), then that set can be used to approximate any desired quantum gate with a short sequence of gates that can also be found efficiently. This theorem is considered one of the most significant results in the field of quantum computation and was first announced by Robert M. Solovay in 1995 and independently proven by Alexei Kitaev in 1997.[1][2] Michael Nielsen and Christopher M. Dawson have noted its importance in the field.[3]

A consequence of this theorem is that a quantum circuit of m constant-qubit gates can be approximated to ε error (in operator norm) by a quantum circuit of $O(m \log^c(m/\varepsilon))$ gates from a desired finite universal gate set (where c is a constant).[4] By comparison, just knowing that a gate set is universal only implies that constant-qubit gates can be approximated by a finite circuit from the gate set, with no bound on its length. So, the Solovay–Kitaev theorem shows that this approximation can be made surprisingly *efficient*, thereby justifying that quantum computers need only implement a finite number of gates to gain the full power of quantum computation.

Statement

Let $\mathcal{G}$ be a finite set of elements in SU(2) containing its own inverses (so $g \in \mathcal{G}$ implies $g^{-1} \in \mathcal{G}$) and such that the group $\langle \mathcal{G} \rangle$ they generate is dense in SU(2). Consider some $\varepsilon > 0$. Then there is a constant c such that for any $U \in \mathrm{SU}(2)$, there is a sequence S of gates from $\mathcal{G}$ of length $O(\log^c(1/\varepsilon))$ such that $\|S - U\| \leq \varepsilon$. That is, S approximates U to operator norm error.[3] Furthermore, there is an efficient algorithm to find such a sequence. More generally, the theorem also holds in SU(d) for any fixed d.

This theorem also holds without the assumption that $\mathcal{G}$ contains its own inverses, although presently with a larger value of c that also increases with the dimension d.[5]

Quantitative bounds

The constant c can be made to be $\log_{(1+\sqrt{5})/2} 2 + \delta = 1.44042\ldots + \delta$ for any fixed $\delta > 0$.[6] However, there exist particular gate sets for which we can take $c = 1$, which makes the length of the gate sequence optimal up to a constant factor.[7]

Proof idea

Every known proof of the fully general Solovay–Kitaev theorem proceeds by recursively constructing a gate sequence giving increasingly good approximations to $U \in \mathrm{SU}(2)$.[3] Suppose we have an approximation $U_{n-1} \in \mathrm{SU}(2)$ such that $\|U - U_{n-1}\| \leq \varepsilon_{n-1}$. Our goal is to find a sequence of gates

approximating UU_{n-1}^{-1} to ε_n error, for $\varepsilon_n < \varepsilon_{n-1}$. By concatenating this sequence of gates with U_{n-1}, we get a sequence of gates U_n such that $\|U - U_n\| \leq \varepsilon_n$.

The main idea in the original argument of Solovay and Kitaev is that commutators of elements close to the identity can be approximated "better-than-expected". Specifically, for $V, W \in \mathrm{SU}(2)$ satisfying $\|V - I\| \leq \delta_1$ and $\|W - I\| \leq \delta_1$ and approximations $\tilde{V}, \tilde{W} \in \mathrm{SU}(2)$ satisfying $\|V - \tilde{V}\| \leq \delta_2$ and $\|W - \tilde{W}\| \leq \delta_2$, then

$$\|VWV^{-1}W^{-1} - \tilde{V}\tilde{W}\tilde{V}^{-1}\tilde{W}^{-1}\| \leq O(\delta_1\delta_2),$$

where the big O notation hides higher-order terms. One can naively bound the above expression to be $O(\delta_2)$, but the group commutator structure creates substantial error cancellation.

We can use this observation to approximate UU_{n-1}^{-1} as a group commutator $V_{n-1}W_{n-1}V_{n-1}^{-1}W_{n-1}^{-1}$. This can be done such that both V_{n-1} and W_{n-1} are close to the identity (since $\|UU_{n-1}^{-1} - I\| \leq \varepsilon_{n-1}$). So, if we recursively compute gate sequences approximating V_{n-1} and W_{n-1} to ε_{n-1} error, we get a gate sequence approximating UU_{n-1}^{-1} to the desired better precision ε_n with ε_n. We can get a base case approximation with constant ε_0 with an exhaustive search of bounded-length gate sequences.

Proof of Solovay-Kitaev Theorem

Let us choose the initial value ε_0 so that $\varepsilon_0 < \varepsilon'$ to be able to apply the iterated “shrinking” lemma. In addition we want $s\varepsilon_0 < 1$ to make sure that ε_k decreases as we increase k. Moreover, we also make sure that ε_0 is small enough so that $\varepsilon_k^2 < \varepsilon_{k+1}$.

Since $\langle G \rangle$ is dense in $\mathrm{SU}(2)$, we can choose l_0 large enough[8] so that G^{l_0} is an ε_0^2-net for $\mathrm{SU}(2)$ (and hence for $\mathrm{S}_{\varepsilon_0}$, as well), no matter how small ε_0 is. Thus, given any $U \in \mathrm{SU}(2)$, we can choose $U_0 \in G^{l_0}$ such that $||U - U_0|| < \varepsilon_0^2$. Let $\Delta := UU_0^+$ be the “difference” of U and U_0. Then

$$\|\Delta_1 - I\| = \|(U - U_0)U_0^+\| = \|U - U_0\| < \varepsilon_0^2 < \varepsilon_1.$$

Hence, $\Delta_1 \in \mathrm{S}_{\varepsilon_1}$. By invoking the iterated "shrinking" lemma with $k = 1$, there exists $U_1 \in G^{l_1}$ such that

$$\|\Delta_1 - U_1\| = \|UU_0^+ - U_1\| = \|U - U_1U_0\| < \varepsilon_1^2.$$

Similarly let $\Delta_2 := \Delta_1 U_1^+ = UU_0^+U_1^+$. Then

$$\|\Delta_2 - I\| = \|(U - U_1U_0)U_0^+U_1^+\| = \|U - U_1U_0\| < \varepsilon_1^2 < \varepsilon_2.$$

Thus, $\Delta_2 \in \mathrm{S}_{\varepsilon_2}$ and we can invoke the iterated "shrinking" lemma (with $k = 2$ this time) to get $U_2 \in G^{l_2}$ such that $\|\Delta_2 - U_2\| = \|UU_0^+U_1^+ - U_2\| = \|U - U_2U_1U_0\| < \varepsilon_2^2$.

If we continue in this way, after k steps we get $U_k \in \mathrm{G}^{l_k}$ such that

$$\|U - U_kU_{k-1}\ldots U_0\| < \varepsilon_k^2.$$

Thus, we have obtained a sequence of

$$L = \sum_{m=0}^{k} l_m = \sum_{m=0}^{k} 5^m l_0 = \frac{5^{k+1}-1}{4} l_0 < \frac{5}{4} 5^k l_0$$

gates that approximates U to accuracy ε_k^2. To determine the value of k, we set $\varepsilon_k^2 = \left((s\varepsilon_0)^{(3/2)^k} / s \right)^2 = \varepsilon$ and solve for k:

$$\left(\frac{3}{2}\right)^k = \frac{\log(1/s^2\varepsilon)}{2\log(1/s\varepsilon_0)}.$$

Now we can always choose ε_0 slightly smaller so that the obtained value of k is an integer.[9] Let $c = \log 5 / \log(3/2) \approx 3.97$ so that $5^k = \left(\frac{3}{2}\right)^{kc}$. Then

$$L < \frac{5}{4} 5^k l_0 = \frac{5}{4} \left(\frac{3}{2}\right)^{kc} l_0 = \frac{5}{4} \left(\frac{\log(1/s^2\varepsilon)}{2\log(1/s\varepsilon_0)} \right)^c l_0$$

Hence for any $U \in \mathrm{SU}(2)$ there is a sequence of $L = O(\log^c(1/\varepsilon))$ gates that approximates U to accuracy ε.

Solovay-Kitaev algorithm for qubits

Here the main ideas that are used in the SK algorithm have been presented. The SK algorithm may be expressed in nine lines of pseudocode. Each of these lines are explained in detail below, but present it here in its entirety both for the reader's reference, and to stress the conceptual simplicity of the algorithm:

```
function Solovay-Kitaev(Gate U, depth n) is
    if (n == 0)
        return Basic Approximation to U
    else
        set U_{n-1} = Solovay-Kitaev(U, n-1)
        set V, W = GC-Decompose(U U_{n-1}^+)
        set V_{n-1} = Solovay-Kitaev(V, n-1)
        set W_{n-1} = Solovay-Kitaev(W, n-1)
        return U_n = V_{n-1} W_{n-1} V_{n-1}^+ W_{n-1}^+ U_{n-1};
end function
```

Let's examine each of these lines in detail. The first line:

```
function Solovay-Kitaev(Gate U, depth n) is
```

indicates that the algorithm is a function with two inputs: an arbitrary single-qubit quantum gate, U, which we desire to approximate, and a non-negative integer, n, which controls the accuracy of the approximation. The function returns a sequence of instructions which approximates U to an accuracy ε_n, where ε_n is a decreasing function of n, so that as n gets larger, the accuracy gets better, with $\varepsilon_n \to 0$ as $n \to \infty$. ε_n is described in detail below.

The `Solovay-Kitaev` function is recursive, so that to obtain an ε_n-approximation to U, it will call itself to obtain ε_{n-1}-approximations to certain unitaries. The recursion terminates at $n = 0$, beyond which no further recursive calls are made:

```
if (n == 0)
    return Basic Approximation to U
```

In order to implement this step it is assumed that a preprocessing stage has been completed which allows one to find a basic ε_0-approximation to arbitrary $U \in \mathrm{SU}(2)$. Since ε_0 is a constant, in principle this preprocessing stage may be accomplished simply by enumerating and storing a large number of instruction sequences from G, say up to some sufficiently large (but fixed) length l_0, and then providing a lookup routine which, given U, returns the closest sequence.

At higher levels of recursion, to find an ε_n-approximation to U, one begins by finding an ε_{n-1}-approximation to U:

```
else
    set U_{n-1} = Solovay-Kitaev(U,n-1)
```

U_{n-1} is used as a step towards finding an improved approximation to U. Defining $\Delta \equiv U U_{n-1}^{+}$, the next three steps of the algorithm aim to find an ε_n-approximation to Δ, where ε_n is some improved level of accuracy, i.e., $\varepsilon_n < \varepsilon_{n-1}$. Finding such an approximation also enables us to obtain an ε_n-approximation to U, simply by concatenating exact sequence of instructions for U_{n-1} with ε_n-approximating sequence for Δ.

How do we find such an approximation to? First, observe that Δ is within a distance ε_{n-1} of the identity. This follows from the definition of Δ and the fact that U_{n-1} is within a distance ε_{n-1} of U.

Second, decompose Δ as a group commutator $\Delta = VWV^{+}W^{+}$ of unitary gates V and W. For any Δ it turns out that this is not obvious and that there is always an infinite set of choices for V and W such that $\Delta = VWV^{+}W^{+}$. For our purposes it is important that we find V and W such that $d(I,V), d(I,W) < c_{gc}\sqrt{\varepsilon_{n-1}}$ for some constant c_{gc}. We call such a decomposition a *balanced group commutator*.

```
set V,W = GC-Decompose(U U_{n-1}^+)
```

For practical implementations we will see below that it is useful to have c_{gc} as small as possible.

The next step is to find instruction sequences which are ε_{n-1}-approximations to V and W:

```
set V_{n-1} = Solovay-Kitaev(V, n-1)

set W_{n-1} = Solovay-Kitaev(W, n-1)
```

The group commutator of V_{n-1} and W_n turns out to be an $\varepsilon_{n-1} \equiv c_{\text{approx}} \varepsilon_{n-1}^{3/2}$-approximation to Δ, for some small constant c_{approx}. Provided $\varepsilon_{n-1} < 1/c_{\text{approx}}^2$, we see that $\varepsilon_n < \varepsilon_{n-1}$, and this procedure therefore provides an improved approximation to Δ, and thus to U.

The constant c_{approx} is important as it determines the precision ε_0 required of the initial approximations. In particular, we see that for this construction to guarantee that $\varepsilon_0 > \varepsilon_1 > \ldots$ we must have $\varepsilon_0 < 1/c_{\text{approx}}^2$.

The algorithm concludes by returning the sequences approximating the group commutator, as well as U_{n-1}:

```
return U_n = V_{n-1} W_{n-1} V_{n-1}^+ W_{n-1}^+ U_{n-1} ;
```

Summing up, the function `Solovay-Kitaev(U, n)` returns a sequence which provides an $\varepsilon_n = c_{\text{approx}} \varepsilon_{n-1}^{3/2}$-approximation to the desired unitary U . The five constituents in this sequence are all obtained by calling the function at the $n-1$th level of recursion.[10]

References

1. Kitaev, A Yu (1997-12-31). "Quantum computations: algorithms and error correction" (https://dx.doi.org/10.1070/rm1997v052n06abeh002155). *Russian Mathematical Surveys*. **52** (6): 1191–1249. Bibcode:1997RuMaS..52.1191K (https://ui.adsabs.harvard.edu/abs/1997RuMaS..52.1191K). doi:10.1070/rm1997v052n06abeh002155 (https://doi.org/10.1070%2Frm1997v052n06abeh002155). ISSN 0036-0279 (https://search.worldcat.org/issn/0036-0279). S2CID 250816585 (https://api.semanticscholar.org/CorpusID:250816585).
2. Kitaev, Alexei Yu.; Shen, Alexander; Vyalyi, Mikhail N. (2002). *Classical and quantum computation* (https://www.worldcat.org/oclc/48965167). Providence, Rhode Island: American Mathematical Society. ISBN 0-8218-2161-X. OCLC 48965167 (https://search.worldcat.org/oclc/48965167).
3. Dawson, Christopher M.; Nielsen, Michael (2006-01-01). "The Solovay-Kitaev algorithm" (https://dl.acm.org/doi/abs/10.5555/2011679.2011685). *Quantum Information & Computation*. **6**: 81–95. arXiv:quant-ph/0505030 (https://arxiv.org/abs/quant-ph/0505030). doi:10.26421/QIC6.1-6 (https://doi.org/10.26421%2FQIC6.1-6).
4. Nielsen, Michael A.; Chuang, Isaac L. (2010). "The Solovay–Kitaev theorem". *Quantum Computation and Quantum Information: 10th Anniversary Edition* (https://www.cambridge.org/core/books/quantum-computation-and-quantum-information/solovaykitaev-theorem/0087DB96E95447C2C6B1C1F61F14D642). pp. 617–624. doi:10.1017/cbo9780511976667.019 (https://doi.org/10.1017%2Fcbo9780511976667.019). ISBN 9780511976667. Retrieved 2020-05-20.
5. Bouland, Adam; Giurgica-Tiron, Tudor (2021-12-03), *Efficient Universal Quantum Compilation: An Inverse-free Solovay-Kitaev Algorithm*, arXiv:2112.02040 (https://arxiv.org/abs/2112.02040)
6. Kuperberg, Greg (2023-06-22), "Breaking the cubic barrier in the Solovay-Kitaev algorithm", arXiv:2306.13158 (https://arxiv.org/abs/2306.13158) [quant-ph (https://arxiv.org/archive/qua

nt-ph)]
7. Ross, Neil J.; Selinger, Peter. "Optimal ancilla-free Clifford+T approximation of z-rotations" (https://www.rintonpress.com/journals/doi/QIC16.11-12-1.html). *Quantum Information & Computation*. **16** (11–12): 901–953. arXiv:1403.2975 (https://arxiv.org/abs/1403.2975). doi:10.26421/QIC16.11-12-1 (https://doi.org/10.26421%2FQIC16.11-12-1).
8. Kitaev, Yu. "Quantum computations: algorithms and error correction" (https://mi.mathnet.ru/eng/umn/v52/i6/p53).
9. Nielsen, Chuang, M.A., I.L. "Quantum Computation and Quantum Information (Cambridge University Press, 2000), Appendix 3, pp. 617{624". `{{cite web}}`: Missing or empty `|url=` (help)
10. CHRISTOPHER M. DAWSON, MICHAEL A. NIELSEN. "THE SOLOVAY-KITAEV ALGORITHM" (https://arxiv.org/pdf/quant-ph/0505030).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Solovay–Kitaev_theorem&oldid=1245358490"

WIKIPEDIA
The Free Encyclopedia

Schrödinger–HJW theorem

In quantum information theory and quantum optics, the **Schrödinger–HJW theorem** is a result about the realization of a mixed state of a quantum system as an ensemble of pure quantum states and the relation between the corresponding purifications of the density operators. The theorem is named after physicists and mathematicians Erwin Schrödinger,[1] Lane P. Hughston, Richard Jozsa and William Wootters.[2] The result was also found independently (albeit partially) by Nicolas Gisin,[3] and by Nicolas Hadjisavvas building upon work by Ed Jaynes,[4][5] while a significant part of it was likewise independently discovered by N. David Mermin.[6] Thanks to its complicated history, it is also known by various other names such as the **GHJW theorem**,[7] the **HJW theorem**, and the **purification theorem**.

Purification of a mixed quantum state

Let $\mathcal{H}_S$ be a finite-dimensional complex Hilbert space, and consider a generic (possibly mixed) quantum state ρ defined on $\mathcal{H}_S$ and admitting a decomposition of the form

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$$

for a collection of (not necessarily mutually orthogonal) states $|\phi_i\rangle \in \mathcal{H}_S$ and coefficients $p_i \geq 0$ such that $\sum_i p_i = 1$. Note that any quantum state can be written in such a way for some $\{|\phi_i\rangle\}_i$ and $\{p_i\}_i$.[8]

Any such ρ can be *purified*, that is, represented as the partial trace of a pure state defined in a larger Hilbert space. More precisely, it is always possible to find a (finite-dimensional) Hilbert space $\mathcal{H}_A$ and a pure state $|\Psi_{SA}\rangle \in \mathcal{H}_S \otimes \mathcal{H}_A$ such that $\rho = \mathrm{Tr}_A\left(|\Psi_{SA}\rangle\langle\Psi_{SA}|\right)$. Furthermore, the states $|\Psi_{SA}\rangle$ satisfying this are all and only those of the form

$$|\Psi_{SA}\rangle = \sum_i \sqrt{p_i}|\phi_i\rangle \otimes |a_i\rangle$$

for some orthonormal basis $\{|a_i\rangle\}_i \subset \mathcal{H}_A$. The state $|\Psi_{SA}\rangle$ is then referred to as the "purification of ρ". Since the auxiliary space and the basis can be chosen arbitrarily, the purification of a mixed state is not unique; in fact, there are infinitely many purifications of a given mixed state.[9] Because all of them admit a decomposition in the form given above, given any pair of purifications $|\Psi\rangle, |\Psi'\rangle \in \mathcal{H}_S \otimes \mathcal{H}_A$, there is always some unitary operation $U : \mathcal{H}_A \to \mathcal{H}_A$ such that

$$|\Psi'\rangle = (I \otimes U)|\Psi\rangle.$$

Theorem

Consider a mixed quantum state ρ with two different realizations as ensemble of pure states as $\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|$ and $\rho = \sum_j q_j|\varphi_j\rangle\langle\varphi_j|$. Here both $|\phi_i\rangle$and $|\varphi_j\rangle$ are not assumed to be mutually orthogonal. There will be two corresponding purifications of the mixed state ρ reading as follows:

Purification 1: $|\Psi_{SA}^1\rangle = \sum_i \sqrt{p_i}|\phi_i\rangle \otimes |a_i\rangle$;

Purification 2: $|\Psi_{SA}^2\rangle = \sum_j \sqrt{q_j}|\varphi_j\rangle \otimes |b_j\rangle$.

The sets $\{|a_i\rangle\}$and $\{|b_j\rangle\}$ are two collections of orthonormal bases of the respective auxiliary spaces. These two purifications only differ by a unitary transformation acting on the auxiliary space, namely, there exists a unitary matrix U_A such that $|\Psi_{SA}^1\rangle = (I \otimes U_A)|\Psi_{SA}^2\rangle$.[10] Therefore, $|\Psi_{SA}^1\rangle = \sum_j \sqrt{q_j}|\varphi_j\rangle \otimes U_A|b_j\rangle$, which means that we can realize the different ensembles of a mixed state just by making different measurements on the purifying system.

References

1. Schrödinger, Erwin (1936). "Probability relations between separated systems". *Proceedings of the Cambridge Philosophical Society*. **32** (3): 446–452. Bibcode:1936PCPS...32..446S (https://ui.adsabs.harvard.edu/abs/1936PCPS...32..446S). doi:10.1017/S0305004100019137 (https://doi.org/10.1017%2FS0305004100019137).
2. Hughston, Lane P.; Jozsa, Richard; Wootters, William K. (November 1993). "A complete classification of quantum ensembles having a given density matrix". *Physics Letters A*. **183** (1): 14–18. Bibcode:1993PhLA..183...14H (https://ui.adsabs.harvard.edu/abs/1993PhLA..183...14H). doi:10.1016/0375-9601(93)90880-9 (https://doi.org/10.1016%2F0375-9601%2893%2990880-9). ISSN 0375-9601 (https://search.worldcat.org/issn/0375-9601).
3. Gisin, N. (1989). “Stochastic quantum dynamics and relativity”, Helvetica Physica Acta 62, 363–371.
4. Hadjisavvas, Nicolas (1981). "Properties of mixtures on non-orthogonal states". *Letters in Mathematical Physics*. **5** (4): 327–332. Bibcode:1981LMaPh...5..327H (https://ui.adsabs.harvard.edu/abs/1981LMaPh...5..327H). doi:10.1007/BF00401481 (https://doi.org/10.1007%2FBF00401481).
5. Jaynes, E. T. (1957). "Information theory and statistical mechanics. II". *Physical Review*. **108** (2): 171–190. Bibcode:1957PhRv..108..171J (https://ui.adsabs.harvard.edu/abs/1957PhRv..108..171J). doi:10.1103/PhysRev.108.171 (https://doi.org/10.1103%2FPhysRev.108.171).
6. Fuchs, Christopher A. (2011). *Coming of Age with Quantum Information: Notes on a Paulian Idea*. Cambridge: Cambridge University Press. ISBN 978-0-521-19926-1. OCLC 535491156 (https://search.worldcat.org/oclc/535491156).
7. Mermin, N. David (1999). "What Do These Correlations Know about Reality? Nonlocality and the Absurd". *Foundations of Physics*. **29** (4): 571–587. arXiv:quant-ph/9807055 (https://arxiv.org/abs/quant-ph/9807055). Bibcode:1998quant.ph..7055M (https://ui.adsabs.harvard.edu/abs/1998quant.ph..7055M). doi:10.1023/A:1018864225930 (https://doi.org/10.1023%2FA%3A1018864225930).
8. Nielsen, Michael A.; Chuang, Isaac L., "The Schmidt decomposition and purifications" (https://doi.org/10.1017/CBO9780511976667.006), *Quantum Computation and Quantum Information*, Cambridge: Cambridge University Press, pp. 110–111.
9. Watrous, John (2018). *The Theory of Quantum Information* (https://www.cambridge.org/core/books/theory-of-quantum-information/AE4AA5638F808D2CFEB070C55431D897). Cambridge: Cambridge University Press. doi:10.1017/9781316848142 (https://doi.org/10.1017%2F9781316848142). ISBN 978-1-107-18056-7.
10. Kirkpatrick, K. A. (February 2006). "The Schrödinger-HJW Theorem". *Foundations of Physics Letters*. **19** (1): 95–102. arXiv:quant-ph/0305068 (https://arxiv.org/abs/quant-ph/0305068). Bibcode:2006FoPhL..19...95K (https://ui.adsabs.harvard.edu/abs/2006FoPhL..19...9

5K). doi:10.1007/s10702-006-1852-1 (https://doi.org/10.1007%2Fs10702-006-1852-1). ISSN 0894-9875 (https://search.worldcat.org/issn/0894-9875).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Schrödinger–HJW_theorem&oldid=1209707817"

WIKIPEDIA
The Free Encyclopedia

Classical capacity

In quantum information theory, the **classical capacity** of a quantum channel is the maximum rate at which classical data can be sent over it error-free in the limit of many uses of the channel. Holevo, Schumacher, and Westmoreland proved the following least upper bound on the classical capacity of any quantum channel $\mathcal{N}$:

$$\chi(\mathcal{N}) = \max_{\rho^{XA}} I(X;B)_{\mathcal{N}(\rho)}$$

where ρ^{XA} is a classical-quantum state of the following form:

$$\rho^{XA} = \sum_x p_X(x)|x\rangle\langle x|^X \otimes \rho_x^A,$$

$p_X(x)$ is a probability distribution, and each ρ_x^A is a density operator that can be input to the channel $\mathcal{N}$.

Achievability using sequential decoding

We briefly review the HSW coding theorem (the statement of the achievability of the Holevo information rate $I(X;B)$ for communicating classical data over a quantum channel). We first review the minimal amount of quantum mechanics needed for the theorem. We then cover quantum typicality, and finally we prove the theorem using a recent sequential decoding technique.

Review of quantum mechanics

In order to prove the HSW coding theorem, we really just need a few basic things from quantum mechanics. First, a quantum state is a unit trace, positive operator known as a density operator. Usually, we denote it by ρ, σ, ω, etc. The simplest model for a quantum channel is known as a classical-quantum channel:

$$x \mapsto \rho_x.$$

The meaning of the above notation is that inputting the classical letter x at the transmitting end leads to a quantum state ρ_x at the receiving end. It is the task of the receiver to perform a measurement to determine the input of the sender. If it is true that the states ρ_x are perfectly distinguishable from one another (i.e., if they have orthogonal supports such that $\operatorname{Tr}\{\rho_x \rho_{x'}\} = 0$ for $x \neq x'$), then the channel is a noiseless channel. We are interested in situations for which this is not the case. If it is true that the states ρ_x all commute with one another, then this is effectively identical to the situation for a classical channel, so we are also not interested in these situations. So, the situation in which we are interested is that in which the states ρ_x have overlapping support and are non-commutative.

The most general way to describe a quantum measurement is with a positive operator-valued measure (POVM). We usually denote the elements of a POVM as $\{\Lambda_m\}_m$. These operators should satisfy positivity and completeness in order to form a valid POVM:

$$\Lambda_m \geq 0 \quad \forall m$$
$$\sum_m \Lambda_m = I.$$

The probabilistic interpretation of quantum mechanics states that if someone measures a quantum state ρ using a measurement device corresponding to the POVM $\{\Lambda_m\}$, then the probability $p(m)$ for obtaining outcome m is equal to

$$p(m) = \operatorname{Tr}\{\Lambda_m \rho\},$$

and the post-measurement state is

$$\rho'_m = \frac{1}{p(m)} \sqrt{\Lambda_m} \rho \sqrt{\Lambda_m},$$

if the person measuring obtains outcome m. These rules are sufficient for us to consider classical communication schemes over cq channels.

Quantum typicality

The reader can find a good review of this topic in the article about the typical subspace.

Gentle operator lemma

The following lemma is important for our proofs. It demonstrates that a measurement that succeeds with high probability on average does not disturb the state too much on average:

Lemma: [Winter] Given an ensemble $\{p_X(x), \rho_x\}$ with expected density operator $\rho \equiv \sum_x p_X(x) \rho_x$, suppose that an operator Λ such that $I \geq \Lambda \geq 0$ succeeds with high probability on the state ρ:

$$\mathrm{Tr}\{\Lambda \rho\} \geq 1 - \epsilon.$$

Then the subnormalized state $\sqrt{\Lambda} \rho_x \sqrt{\Lambda}$ is close in expected trace distance to the original state ρ_x:

$$\mathbb{E}_X \left\{ \left\| \sqrt{\Lambda} \rho_X \sqrt{\Lambda} - \rho_X \right\|_1 \right\} \leq 2\sqrt{\epsilon}.$$

(Note that $\|A\|_1$ is the nuclear norm of the operator A so that $\|A\|_1 \equiv \mathrm{Tr}\left\{\sqrt{A^\dagger A}\right\}$.)

The following inequality is useful for us as well. It holds for any operators ρ, σ, Λ such that $0 \leq \rho, \sigma, \Lambda \leq I$:

$$\mathrm{Tr}\{\Lambda \rho\} \leq \mathrm{Tr}\{\Lambda \sigma\} + \|\rho - \sigma\|_1. \quad (1)$$

The quantum information-theoretic interpretation of the above inequality is that the probability of obtaining outcome Λ from a quantum measurement acting on the state ρ is upper bounded by the probability of obtaining outcome Λ on the state σ summed with the distinguishability of the two states ρ and σ.

Non-commutative union bound

Lemma: [Sen's bound] The following bound holds for a subnormalized state σ such that $0 \leq \sigma$ and $Tr\{\sigma\} \leq 1$ with Π_1, ... , Π_N being projectors: $\mathrm{Tr}\{\sigma\} - \mathrm{Tr}\{\Pi_N \cdots \Pi_1 \, \sigma \, \Pi_1 \cdots \Pi_N\} \leq 2\sqrt{\sum_{i=1}^N \mathrm{Tr}\{(I - \Pi_i)\sigma\}},$

We can think of Sen's bound as a "non-commutative union bound" because it is analogous to the following union bound from probability theory:

$$\Pr\{(A_1 \cap \cdots \cap A_N)^c\} = \Pr\{A_1^c \cup \cdots \cup A_N^c\} \leq \sum_{i=1}^N \Pr\{A_i^c\},$$

where $A_1, \ldots, A_N$ are events. The analogous bound for projector logic would be

$$\mathrm{Tr}\{(I - \Pi_1 \cdots \Pi_N \cdots \Pi_1)\rho\} \leq \sum_{i=1}^N \mathrm{Tr}\{(I - \Pi_i)\rho\},$$

if we think of $\Pi_1 \cdots \Pi_N$ as a projector onto the intersection of subspaces. Though, the above bound only holds if the projectors Π_1, ..., Π_N are commuting (choosing $\Pi_1 = |+\rangle\langle+|$, $\Pi_2 = |0\rangle\langle 0|$, and $\rho = |0\rangle\langle 0|$ gives a counterexample). If the projectors are non-commuting, then Sen's bound is the next best thing and suffices for our purposes here.

HSW theorem with the non-commutative union bound

We now prove the HSW theorem with Sen's non-commutative union bound. We divide up the proof into a few parts: codebook generation, POVM construction, and error analysis.

Codebook Generation. We first describe how Alice and Bob agree on a random choice of code. They have the channel $x \to \rho_x$ and a distribution $p_X(x)$. They choose M classical sequences x^n according to the IID\ distribution $p_{X^n}(x^n)$. After selecting them, they label them with indices as $\{x^n(m)\}_{m\in[M]}$. This leads to the following quantum codewords:

$$\rho_{x^n(m)} = \rho_{x_1(m)} \otimes \cdots \otimes \rho_{x_n(m)}.$$

The quantum codebook is then $\{\rho_{x^n(m)}\}$. The average state of the codebook is then

$$\mathbb{E}_{X^n}\{\rho_{X^n}\} = \sum_{x^n} p_{X^n}(x^n)\,\rho_{x^n} = \rho^{\otimes n}, \tag{2}$$

where $\rho = \sum_x p_X(x)\,\rho_x$.

POVM Construction . Sens' bound from the above lemma suggests a method for Bob to decode a state that Alice transmits. Bob should first ask "Is the received state in the average typical subspace?" He can do this operationally by performing a typical subspace measurement corresponding to $\{\Pi^n_{\rho,\delta}, I - \Pi^n_{\rho,\delta}\}$. Next, he asks in sequential order, "Is the received codeword in the m^{th} conditionally typical subspace?" This is in some sense equivalent to the question, "Is the received codeword the m^{th} transmitted codeword?" He can ask these questions operationally by performing the measurements corresponding to the conditionally typical projectors $\{\Pi_{\rho_{x^n(m)},\delta}, I - \Pi_{\rho_{x^n(m)},\delta}\}$.

Why should this sequential decoding scheme work well? The reason is that the transmitted codeword lies in the typical subspace on average:

$$\begin{aligned}
&\mathbb{E}_{X^n}\{\mathrm{Tr}\{\Pi_{\rho,\delta}\,\rho_{X^n}\}\} = \mathrm{Tr}\{\Pi_{\rho,\delta}\,\mathbb{E}_{X^n}\{\rho_{X^n}\}\} \\
&= \mathrm{Tr}\{\Pi_{\rho,\delta}\,\rho^{\otimes n}\} \\
&\geq 1-\epsilon,
\end{aligned}$$

where the inequality follows from (\ref{eq:1st-typ-prop}). Also, the projectors $\Pi_{\rho_{x^n(m)},\delta}$ are "good detectors" for the states $\rho_{x^n(m)}$ (on average) because the following condition holds from conditional quantum typicality:

$$\mathbb{E}_{X^n}\{\mathrm{Tr}\{\Pi_{\rho_{X^n},\delta}\,\rho_{X^n}\}\} \geq 1-\epsilon.$$

Error Analysis. The probability of detecting the m^{th} codeword correctly under our sequential decoding scheme is equal to

$$\mathrm{Tr}\left\{\Pi_{\rho_{X^n(m)},\delta}\hat{\Pi}_{\rho_{X^n(m-1)},\delta}\cdots\hat{\Pi}_{\rho_{X^n(1)},\delta}\,\Pi^n_{\rho,\delta}\,\rho_{x^n(m)}\,\Pi^n_{\rho,\delta}\,\hat{\Pi}_{\rho_{X^n(1)},\delta}\cdots\hat{\Pi}_{\rho_{X^n(m-1)},\delta}\Pi_{\rho_{X^n(m)},\delta}\right\},$$

where we make the abbreviation $\hat{\Pi} \equiv I - \Pi$. (Observe that we project into the average typical subspace just once.) Thus, the probability of an incorrect detection for the m^{th} codeword is given by

$$1 - \mathrm{Tr}\left\{\Pi_{\rho_{X^n(m)},\delta}\hat{\Pi}_{\rho_{X^n(m-1)},\delta}\cdots\hat{\Pi}_{\rho_{X^n(1)},\delta}\,\Pi^n_{\rho,\delta}\,\rho_{x^n(m)}\,\Pi^n_{\rho,\delta}\,\hat{\Pi}_{\rho_{X^n(1)},\delta}\cdots\hat{\Pi}_{\rho_{X^n(m-1)},\delta}\Pi_{\rho_{X^n(m)},\delta}\right\},$$

and the average error probability of this scheme is equal to

$$1 - \frac{1}{M}\sum_m \mathrm{Tr}\left\{\Pi_{\rho_{X^n(m)},\delta}\hat{\Pi}_{\rho_{X^n(m-1)},\delta}\cdots\hat{\Pi}_{\rho_{X^n(1)},\delta}\,\Pi^n_{\rho,\delta}\,\rho_{x^n(m)}\,\Pi^n_{\rho,\delta}\,\hat{\Pi}_{\rho_{X^n(1)},\delta}\cdots\hat{\Pi}_{\rho_{X^n(m-1)},\delta}\Pi_{\rho_{X^n(m)},\delta}\right\}.$$

Instead of analyzing the average error probability, we analyze the expectation of the average error probability, where the expectation is with respect to the random choice of code:

$$1 - \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(m)},\delta} \hat{\Pi}_{\rho_{X^n(m-1)},\delta} \cdots \hat{\Pi}_{\rho_{X^n(1)},\delta} \, \Pi^n_{\rho,\delta} \, \rho_{X^n(m)} \, \Pi^n_{\rho,\delta} \, \hat{\Pi}_{\rho_{X^n(1)},\delta} \cdots \hat{\Pi}_{\rho_{X^n(m-1)},\delta} \Pi_{\rho_{X^n(m)},\delta} \right\} \right\}. \quad (3)$$

Our first step is to apply Sen's bound to the above quantity. But before doing so, we should rewrite the above expression just slightly, by observing that

$$\begin{aligned}
1 &= \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \rho_{X^n(m)} \right\} \right\} \\
&= \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi^n_{\rho,\delta} \rho_{X^n(m)} \right\} + \operatorname{Tr} \left\{ \hat{\Pi}^n_{\rho,\delta} \rho_{X^n(m)} \right\} \right\} \\
&= \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} + \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \hat{\Pi}^n_{\rho,\delta} \mathbb{E}_{X^n} \left\{ \rho_{X^n(m)} \right\} \right\} \\
&= \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} + \operatorname{Tr} \left\{ \hat{\Pi}^n_{\rho,\delta} \rho^{\otimes n} \right\} \\
&\leq \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} + \epsilon
\end{aligned}$$

Substituting into (3) (and forgetting about the small ϵ term for now) gives an upper bound of

$$\begin{aligned}
&\mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} \\
&- \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(m)},\delta} \hat{\Pi}_{\rho_{X^n(m-1)},\delta} \cdots \hat{\Pi}_{\rho_{X^n(1)},\delta} \, \Pi^n_{\rho,\delta} \, \rho_{X^n(m)} \, \Pi^n_{\rho,\delta} \, \hat{\Pi}_{\rho_{X^n(1)},\delta} \cdots \hat{\Pi}_{\rho_{X^n(m-1)},\delta} \Pi_{\rho_{X^n(m)},\delta} \right\} \right\}.
\end{aligned}$$

We then apply Sen's bound to this expression with $\sigma = \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta}$ and the sequential projectors as $\Pi_{\rho_{X^n(m)},\delta}$, $\hat{\Pi}_{\rho_{X^n(m-1)},\delta}$, ..., $\hat{\Pi}_{\rho_{X^n(1)},\delta}$. This gives the upper bound $\mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m 2 \left[\operatorname{Tr} \left\{ \left(I - \Pi_{\rho_{X^n(m)},\delta} \right) \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} + \sum_{i=1}^{m-1} \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(i)},\delta} \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right]^{1/2} \right\}$. Due to concavity of the square root, we can bound this expression from above by

$$\begin{aligned}
&2 \left[\mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \left(I - \Pi_{\rho_{X^n(m)},\delta} \right) \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} + \sum_{i=1}^{m-1} \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(i)},\delta} \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} \right]^{1/2} \\
&\leq 2 \left[\mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \left(I - \Pi_{\rho_{X^n(m)},\delta} \right) \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} + \sum_{i \neq m} \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(i)},\delta} \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} \right]^{1/2},
\end{aligned}$$

where the second bound follows by summing over all of the codewords not equal to the m^{th} codeword (this sum can only be larger).

We now focus exclusively on showing that the term inside the square root can be made small. Consider the first term:

$$\begin{aligned}
&\mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \left(I - \Pi_{\rho_{X^n(m)},\delta} \right) \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\} \right\} \\
&\leq \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \left(I - \Pi_{\rho_{X^n(m)},\delta} \right) \rho_{X^n(m)} \right\} + \left\| \rho_{X^n(m)} - \Pi^n_{\rho,\delta} \rho_{X^n(m)} \Pi^n_{\rho,\delta} \right\|_1 \right\} \\
&\leq \epsilon + 2\sqrt{\epsilon}.
\end{aligned}$$

where the first inequality follows from (**1**) and the second inequality follows from the gentle operator lemma and the properties of unconditional and conditional typicality. Consider now the second term and the following chain of inequalities:

$$\begin{aligned}
&\sum_{i \neq m} \mathbb{E}_{X^n} \left\{ \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(i)},\delta} \, \Pi^n_{\rho,\delta} \, \rho_{X^n(m)} \, \Pi^n_{\rho,\delta} \right\} \right\} \\
&= \sum_{i \neq m} \operatorname{Tr} \left\{ \mathbb{E}_{X^n} \left\{ \Pi_{\rho_{X^n(i)},\delta} \right\} \, \Pi^n_{\rho,\delta} \, \mathbb{E}_{X^n} \left\{ \rho_{X^n(m)} \right\} \, \Pi^n_{\rho,\delta} \right\} \\
&= \sum_{i \neq m} \operatorname{Tr} \left\{ \mathbb{E}_{X^n} \left\{ \Pi_{\rho_{X^n(i)},\delta} \right\} \, \Pi^n_{\rho,\delta} \, \rho^{\otimes n} \, \Pi^n_{\rho,\delta} \right\} \\
&\leq \sum_{i \neq m} 2^{-n[H(B)-\delta]} \operatorname{Tr} \left\{ \mathbb{E}_{X^n} \left\{ \Pi_{\rho_{X^n(i)},\delta} \right\} \, \Pi^n_{\rho,\delta} \right\}
\end{aligned}$$

The first equality follows because the codewords $X^n\left(m\right)$ and $X^n\left(i\right)$ are independent since they are different. The second equality follows from (**2**). The first inequality follows from (\ref{eq:3rd-typ-prop}). Continuing, we have

$$\begin{aligned}
&\leq \sum_{i \neq m} 2^{-n[H(B)-\delta]} \, \mathbb{E}_{X^n} \left\{ \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(i)},\delta} \right\} \right\} \\
&\leq \sum_{i \neq m} 2^{-n[H(B)-\delta]} \, 2^{n[H(B|X)+\delta]} \\
&= \sum_{i \neq m} 2^{-n[I(X;B)-2\delta]} \\
&\leq M \, 2^{-n[I(X;B)-2\delta]}.
\end{aligned}$$

The first inequality follows from $\Pi^n_{\rho,\delta} \leq I$ and exchanging the trace with the expectation. The second inequality follows from (\ref{eq:2nd-cond-typ}). The next two are straightforward.

Putting everything together, we get our final bound on the expectation of the average error probability:

$$\begin{aligned}
&1 - \mathbb{E}_{X^n} \left\{ \frac{1}{M} \sum_m \operatorname{Tr} \left\{ \Pi_{\rho_{X^n(m)},\delta} \hat{\Pi}_{\rho_{X^n(m-1)},\delta} \cdots \hat{\Pi}_{\rho_{X^n(1)},\delta} \, \Pi^n_{\rho,\delta} \, \rho_{X^n(m)} \, \Pi^n_{\rho,\delta} \, \hat{\Pi}_{\rho_{X^n(1)},\delta} \cdots \hat{\Pi}_{\rho_{X^n(m-1)},\delta} \Pi_{\rho_{X^n(m)},\delta} \right\} \right\} \\
&\leq \epsilon + 2 \left[\left(\epsilon + 2\sqrt{\epsilon} \right) + M \, 2^{-n[I(X;B)-2\delta]} \right]^{1/2}.
\end{aligned}$$

Thus, as long as we choose $M = 2^{n[I(X;B)-3\delta]}$, there exists a code with vanishing error probability.

See also

- Entanglement-assisted classical capacity
- Quantum capacity
- Quantum information theory
- Typical subspace

References

- Holevo, Alexander S. (1998), "The Capacity of Quantum Channel with General Signal States", *IEEE Transactions on Information Theory*, **44** (1): 269–273, arXiv:quant-ph/9611023 (https://arxiv.org/abs/quant-ph/9611023), doi:10.1109/18.651037 (https://doi.org/10.1109%2F18.651037).
- Schumacher, Benjamin; Westmoreland, Michael (1997), "Sending classical information via noisy quantum channels", *Phys. Rev. A*, **56** (1): 131–138, Bibcode:1997PhRvA..56..131S (https://ui.adsabs.harvard.edu/abs/1997PhRvA..56..131S), doi:10.1103/PhysRevA.56.131 (https://doi.org/10.1103%2FPhysRevA.56.131).
- Wilde, Mark M. (2017), *Quantum Information Theory*, Cambridge University Press, arXiv:1106.1445 (https://arxiv.org/abs/1106.1445), Bibcode:2011arXiv1106.1445W (https://ui.adsabs.harvard.edu/abs/2011arXiv1106.1445W), doi:10.1017/9781316809976.001 (https://doi.org/10.1017%2F9781316809976.001), S2CID 2515538 (https://api.semanticscholar.org/CorpusID:2515538)

- Sen, Pranab (2012), "Achieving the Han-Kobayashi inner bound for the quantum interference channel by sequential decoding", *IEEE International Symposium on Information Theory Proceedings (ISIT 2012)*, pp. 736–740, arXiv:1109.0802 (https://arxiv.org/abs/1109.0802), doi:10.1109/ISIT.2012.6284656 (https://doi.org/10.1109%2FISIT.2012.6284656), S2CID 15119225 (https://api.semanticscholar.org/CorpusID:15119225).
- Guha, Saikat; Tan, Si-Hui; Wilde, Mark M. (2012), "Explicit capacity-achieving receivers for optical communication and quantum reading", *IEEE International Symposium on Information Theory Proceedings (ISIT 2012)*, pp. 551–555, arXiv:1202.0518 (https://arxiv.org/abs/1202.0518), doi:10.1109/ISIT.2012.6284251 (https://doi.org/10.1109%2FISIT.2012.6284251), ISBN 978-1-4673-2579-0, S2CID 8786400 (https://api.semanticscholar.org/CorpusID:8786400).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Classical_capacity&oldid=1223170948"

WIKIPEDIA
The Free Encyclopedia

Entanglement-assisted classical capacity

In the theory of quantum communication, the **entanglement-assisted classical capacity** of a quantum channel is the highest rate at which classical information can be transmitted from a sender to receiver when they share an unlimited amount of noiseless entanglement. It is given by the quantum mutual information of the channel, which is the input-output quantum mutual information maximized over all pure bipartite quantum states with one system transmitted through the channel. This formula is the natural generalization of Shannon's noisy channel coding theorem, in the sense that this formula is equal to the capacity, and there is no need to regularize it. An additional feature that it shares with Shannon's formula is that a noiseless classical or quantum feedback channel cannot increase the entanglement-assisted classical capacity. The entanglement-assisted classical capacity theorem is proved in two parts: the direct coding theorem and the converse theorem. The direct coding theorem demonstrates that the quantum mutual information of the channel is an achievable rate, by a random coding strategy that is effectively a noisy version of the super-dense coding protocol. The converse theorem demonstrates that this rate is optimal by making use of the strong subadditivity of quantum entropy.

See also

- Classical capacity
- Quantum capacity
- Typical subspace

References

- Christoph Adami and Nicolas J. Cerf. von Neumann capacity of noisy quantum channels. Physical Review A, 56(5):3470-3483, November 1997.
- Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. Physical Review Letters, 83(15):3081-3084, October 1999.
- Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. IEEE Transactions on Information Theory, 48:2637-2655, 2002.
- Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Physical Review Letters, 69(20):2881-2884, November 1992.
- Garry Bowen. Quantum feedback channels. IEEE Transactions on Information Theory, 50(10):2429-2434, October 2004. arXiv:quant-ph/0209076 (https://arxiv.org/abs/quant-ph/0209076).
- Wilde, Mark M. (2013), *Quantum Information Theory*, Cambridge University Press, arXiv:1106.1445 (https://arxiv.org/abs/1106.1445), doi:10.1017/9781316809976.001 (https://doi.org/10.1017%2F9781316809976.001), S2CID 2515538 (https://api.semanticscholar.org/CorpusID:2515538)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Entanglement-assisted_classical_capacity&oldid=1087469573"

WIKIPEDIA
The Free Encyclopedia

Quantum capacity

In the theory of quantum communication, the **quantum capacity** is the highest rate at which quantum information can be communicated over many independent uses of a noisy quantum channel from a sender to a receiver. It is also equal to the highest rate at which entanglement can be generated over the channel, and forward classical communication cannot improve it. The quantum capacity theorem is important for the theory of quantum error correction, and more broadly for the theory of quantum computation. The theorem giving a lower bound on the quantum capacity of any channel is colloquially known as the LSD theorem, after the authors Lloyd,[1] Shor,[2] and Devetak[3] who proved it with increasing standards of rigor.[4]

Hashing bound for Pauli channels

The LSD theorem states that the coherent information of a quantum channel is an achievable rate for reliable quantum communication. For a Pauli channel, the coherent information has a simple form and the proof that it is achievable is particularly simple as well. We prove the theorem for this special case by exploiting random stabilizer codes and correcting only the likely errors that the channel produces.

Theorem (hashing bound). There exists a stabilizer quantum error-correcting code that achieves the hashing limit $R = 1 - H(\mathbf{p})$ for a Pauli channel of the following form:

$$\rho \mapsto p_I \rho + p_X X\rho X + p_Y Y\rho Y + p_Z Z\rho Z,$$

where $\mathbf{p} = (p_I, p_X, p_Y, p_Z)$ and $H(\mathbf{p})$ is the entropy of this probability vector.

Proof. Consider correcting only the typical errors. That is, consider defining the typical set of errors as follows:

$$T_\delta^{\mathbf{p}^n} \equiv \left\{ a^n : \left| -\frac{1}{n}\log_2(\Pr\{E_{a^n}\}) - H(\mathbf{p}) \right| \leq \delta \right\},$$

where a^n is some sequence consisting of the letters $\{I, X, Y, Z\}$ and $\Pr\{E_{a^n}\}$ is the probability that an IID Pauli channel issues some tensor-product error $E_{a^n} \equiv E_{a_1} \otimes \cdots \otimes E_{a_n}$. This typical set consists of the likely errors in the sense that

$$\sum_{a^n \in T_\delta^{\mathbf{p}^n}} \Pr\{E_{a^n}\} \geq 1 - \epsilon,$$

for all $\epsilon > 0$ and sufficiently large n. The error-correcting conditions[5] for a stabilizer code $\mathcal{S}$ in this case are that $\{E_{a^n} : a^n \in T_\delta^{\mathbf{p}^n}\}$ is a correctable set of errors if

$$E_{a^n}^\dagger E_{b^n} \notin N(\mathcal{S}) \backslash \mathcal{S},$$

for all error pairs E_{a^n} and E_{b^n} such that $a^n, b^n \in T_\delta^{\mathbf{p}^n}$ where $N(\mathcal{S})$ is the normalizer of $\mathcal{S}$. Also, we consider the expectation of the error probability under a random choice of a stabilizer code.

Proceed as follows:

$$\begin{aligned}
\mathbb{E}_{\mathcal{S}}\left\{p_e\right\} &= \mathbb{E}_{\mathcal{S}}\left\{\sum_{a^n} \Pr\left\{E_{a^n}\right\} \mathcal{I}\left(E_{a^n} \text{ is uncorrectable under } \mathcal{S}\right)\right\} \\
&\leq \mathbb{E}_{\mathcal{S}}\left\{\sum_{a^n \in T_\delta^{\mathbf{p}^n}} \Pr\left\{E_{a^n}\right\} \mathcal{I}\left(E_{a^n} \text{ is uncorrectable under } \mathcal{S}\right)\right\} + \epsilon \\
&= \sum_{a^n \in T_\delta^{\mathbf{p}^n}} \Pr\left\{E_{a^n}\right\} \mathbb{E}_{\mathcal{S}}\left\{\mathcal{I}\left(E_{a^n} \text{ is uncorrectable under } \mathcal{S}\right)\right\} + \epsilon \\
&= \sum_{a^n \in T_\delta^{\mathbf{p}^n}} \Pr\left\{E_{a^n}\right\} \Pr_{\mathcal{S}}\left\{E_{a^n} \text{ is uncorrectable under } \mathcal{S}\right\} + \epsilon.
\end{aligned}$$

The first equality follows by definition—$\mathcal{I}$ is an indicator function equal to one if E_{a^n} is uncorrectable under $\mathcal{S}$ and equal to zero otherwise. The first inequality follows, since we correct only the typical errors because the atypical error set has negligible probability mass. The second equality follows by exchanging the expectation and the sum. The third equality follows because the expectation of an indicator function is the probability that the event it selects occurs.

Continuing, we have:

$$\begin{aligned}
&= \sum_{a^n \in T_\delta^{\mathbf{p}^n}} \Pr\left\{E_{a^n}\right\} \Pr_{\mathcal{S}}\left\{\exists E_{b^n} : b^n \in T_\delta^{\mathbf{p}^n},\ b^n \neq a^n,\ E_{a^n}^\dagger E_{b^n} \in N\left(\mathcal{S}\right) \backslash \mathcal{S}\right\} \\
&\leq \sum_{a^n \in T_\delta^{A^n}} \Pr\left\{E_{a^n}\right\} \Pr_{\mathcal{S}}\left\{\exists E_{b^n} : b^n \in T_\delta^{\mathbf{p}^n},\ b^n \neq a^n,\ E_{a^n}^\dagger E_{b^n} \in N\left(\mathcal{S}\right)\right\} \\
&= \sum_{a^n \in T_\delta^{\mathbf{p}^n}} \Pr\left\{E_{a^n}\right\} \Pr_{\mathcal{S}}\left\{\bigcup_{b^n \in T_\delta^{\mathbf{p}^n},\, b^n \neq a^n} E_{a^n}^\dagger E_{b^n} \in N\left(\mathcal{S}\right)\right\} \\
&\leq \sum_{a^n, b^n \in T_\delta^{\mathbf{p}^n},\, b^n \neq a^n} \Pr\left\{E_{a^n}\right\} \Pr_{\mathcal{S}}\left\{E_{a^n}^\dagger E_{b^n} \in N\left(\mathcal{S}\right)\right\} \\
&\leq \sum_{a^n, b^n \in T_\delta^{\mathbf{p}^n},\, b^n \neq a^n} \Pr\left\{E_{a^n}\right\} 2^{-(n-k)} \\
&\leq 2^{2n[H(\mathbf{p})+\delta]} 2^{-n[H(\mathbf{p})+\delta]} 2^{-(n-k)} \\
&= 2^{-n[1-H(\mathbf{p})-k/n-3\delta]}.
\end{aligned}$$

The first equality follows from the error-correcting conditions for a quantum stabilizer code, where $N\left(\mathcal{S}\right)$ is the normalizer of $\mathcal{S}$. The first inequality follows by ignoring any potential degeneracy in the code—we consider an error uncorrectable if it lies in the normalizer $N\left(\mathcal{S}\right)$ and the probability can only be larger because $N\left(\mathcal{S}\right) \backslash \mathcal{S} \in N\left(\mathcal{S}\right)$. The second equality follows by realizing that the probabilities for the existence criterion and the union of events are equivalent. The second inequality follows by applying the union bound. The third inequality follows from the fact that the probability for a fixed operator $E_{a^n}^\dagger E_{b^n}$ not equal to the identity commuting with the stabilizer operators of a random stabilizer can be

upper bounded as follows: $\Pr_{\mathcal{S}}\left\{E_{a^n}^{\dagger}E_{b^n}\in N\left(\mathcal{S}\right)\right\}=\frac{2^{n+k}-1}{2^{2n}-1}\leq 2^{-(n-k)}$. The reasoning here is that the random choice of a stabilizer code is equivalent to fixing operators Z_1, ..., Z_{n-k} and performing a uniformly random Clifford unitary. The probability that a fixed operator commutes with $\overline{Z}_1$, ..., $\overline{Z}_{n-k}$ is then just the number of non-identity operators in the normalizer ($2^{n+k}-1$) divided by the total number of non-identity operators ($2^{2n}-1$). After applying the above bound, we then exploit the following typicality bounds:

$$\forall a^n\in T_{\delta}^{\mathbf{p}^n}:\Pr\left\{E_{a^n}\right\}\leq 2^{-n[H(\mathbf{p})+\delta]},$$
$$\left|T_{\delta}^{\mathbf{p}^n}\right|\leq 2^{n[H(\mathbf{p})+\delta]}.$$

We conclude that as long as the rate $k/n=1-H\left(\mathbf{p}\right)-4\delta$, the expectation of the error probability becomes arbitrarily small, so that there exists at least one choice of a stabilizer code with the same bound on the error probability.

See also

- Quantum computing

References

1. Seth Lloyd (1997). "Capacity of the noisy quantum channel". *Physical Review A*. **55** (3): 1613–1622. arXiv:quant-ph/9604015 (https://arxiv.org/abs/quant-ph/9604015). Bibcode:1997PhRvA..55.1613L (https://ui.adsabs.harvard.edu/abs/1997PhRvA..55.1613L). doi:10.1103/PhysRevA.55.1613 (https://doi.org/10.1103%2FPhysRevA.55.1613). S2CID 5555850 (https://api.semanticscholar.org/CorpusID:5555850).
2. Peter Shor (2002). "The quantum channel capacity and coherent information" (http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/meta/aux/shor.pdf) (PDF). *Lecture Notes, MSRI Workshop on Quantum Computation*.
3. Igor Devetak (2005). "The private classical capacity and quantum capacity of a quantum channel". *IEEE Transactions on Information Theory*. **51**: 44–55. arXiv:quant-ph/0304127 (https://arxiv.org/abs/quant-ph/0304127). doi:10.1109/TIT.2004.839515 (https://doi.org/10.1109%2FTIT.2004.839515). S2CID 12246393 (https://api.semanticscholar.org/CorpusID:12246393).
4. Wilde, Mark M. (2017). *Quantum information theory* (https://www.worldcat.org/oclc/972292559) (2nd ed.). Cambridge, UK. ISBN 978-1-316-80997-6. OCLC 972292559 (https://search.worldcat.org/oclc/972292559).
5. Nielsen, Michael A.; Chuang, Isaac L. (2000), *Quantum Computation and Quantum Information*, Cambridge University Press, ISBN 978-0-521-63503-5.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_capacity&oldid=1119381853"

WIKIPEDIA
The Free Encyclopedia

Entanglement distillation

Entanglement distillation (also called *entanglement purification*) is the transformation of *N* copies of an arbitrary entangled state ρ into some number of approximately pure Bell pairs, using only local operations and classical communication.

Quantum entanglement distillation can in this way overcome the degenerative influence of noisy quantum channels[1] by transforming previously shared less entangled pairs into a smaller number of maximally entangled pairs.

History

The limits for entanglement dilution and distillation are due to C. H. Bennett, H. Bernstein, S. Popescu, and B. Schumacher,[2] who presented the first distillation protocols for pure states in 1996; entanglement distillation protocols for mixed states were introduced by Bennett, Brassard, Popescu, Schumacher, Smolin and Wootters[3] the same year. Bennett, DiVincenzo, Smolin and Wootters[1] established the connection to quantum error-correction in a ground-breaking paper published in August 1996, also in the journal of Physical Review, which has stimulated a lot of subsequent research.

Quantifying entanglement

A two qubit system can be written as a superposition of possible computational basis qubit states: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, each with an associated complex coefficient α:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

As in the case of a single qubit, the probability of measuring a particular computational basis state $|x\rangle$ is the square of the modulus of its amplitude, or associated coefficient, $|\alpha_x|^2$, subject to the normalization condition $\sum_{x\in 0,1} |\alpha_x|^2 = 1$. The normalization condition guarantees that the sum of the probabilities add up to 1, meaning that upon measurement, one of the states will be observed.

The Bell state is a particularly important example of a two qubit state: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Bell states possess the property that measurement outcomes on the two qubits are correlated. As can be seen from the expression above, the two possible measurement outcomes are zero and one, both with probability of 50%. As a result, a measurement of the second qubit always gives the same result as the measurement of the first qubit.

Bell states can be used to quantify entanglement. Let *m* be the number of high-fidelity copies of a Bell state that can be produced using local operations and classical communication (LOCC). Given a large number of Bell states the amount of entanglement present in a pure state $|\psi\rangle$ can then be defined as the ratio of n/m, called the distillable entanglement of a particular state $|\phi\rangle$, which gives a quantified

measure of the amount of entanglement present in a given system. The process of entanglement distillation aims to saturate this limiting ratio. The number of copies of a pure state that may be converted into a maximally entangled state is equal to the von Neumann entropy $S(p)$ of the state, which is an extension of the concept of classical entropy for quantum systems. Mathematically, for a given density matrix p, the von Neumann entropy $S(p)$ is $S(p) = -\mathrm{Tr}(p \ln p)$. Entanglement can then be quantified as the entropy of entanglement, which is the von Neumann entropy of either p_A or p_B as:

$$E = -\mathrm{Tr}(p_A \ln p_A) = -\mathrm{Tr}(p_B \ln p_B),$$

Which ranges from 0 for a product state to $\ln 2$ for a maximally entangled state (if the $\ln$ is replaced by $\log_2$ then maximally entangled has a value of 1).

Motivation

Suppose that two parties, Alice and Bob, would like to communicate classical information over a noisy quantum channel. Either classical or quantum information can be transmitted over a quantum channel by encoding the information in a quantum state. With this knowledge, Alice encodes the classical information that she intends to send to Bob in a (quantum) product state, as a tensor product of reduced density matrices $p_1 \otimes p_2 \otimes \cdots$ where each p is diagonal and can only be used as a one time input for a particular channel ϵ.

The fidelity of the noisy quantum channel is a measure of how closely the output of a quantum channel resembles the input, and is therefore a measure of how well a quantum channel preserves information. If a pure state ψ is sent into a quantum channel emerges as the state represented by density matrix p, the fidelity of transmission is defined as $F = \langle \psi | p | \psi \rangle$.

The problem that Alice and Bob now face is that quantum communication over large distances depends upon successful distribution of highly entangled quantum states, and due to unavoidable noise in quantum communication channels, the quality of entangled states generally decreases exponentially with channel length as a function of the fidelity of the channel. Entanglement distillation addresses this problem of maintaining a high degree of entanglement between distributed quantum states by transforming N copies of an arbitrary entangled state ρ into approximately $S(\rho)N$ Bell pairs, using only local operations and classical communication. The objective is to share strongly correlated qubits between distant parties (Alice and Bob) in order to allow reliable quantum teleportation or quantum cryptography.

Entanglement concentration

Pure states

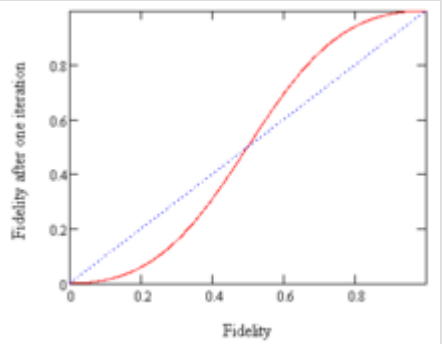
Given n particles in the singlet state shared between Alice and Bob, local actions and classical communication will suffice to prepare m arbitrarily good copies of ϕ with a yield

$$\frac{m}{n} \to \frac{1}{E(\phi)} \text{ as } n \to \infty.$$

Let an entangled state $|\psi\rangle$ have a Schmidt decomposition:

$$|\psi\rangle = \sum_x \sqrt{p(x)}|x_A\rangle|x_B\rangle$$

where coefficients p(x) form a probability distribution, and thus are positive valued and sum to unity. The tensor product of this state is then,



The new fidelity after one iteration of the distillation protocol for pure states.

$$|\psi\rangle^{\otimes m} = \sum_{x_1, x_2, \ldots, x_m} \sqrt{p(x_1)p(x_2)\ldots p(x_m)}|x_{1A}x_{2A}\ldots x_{mA}\rangle|x_{1B}x_{2B}\ldots x_{mB}\rangle$$

Now, omitting all terms $x_1, \ldots, x_m$ which are not part of any sequence which is likely to occur with high probability, known as the typical set: $A_\epsilon^{(n)}$ the new state is

$$|\phi_m\rangle = \sum_{x \epsilon A_\epsilon^{(n)}} \sqrt{p(x_1)p(x_2)\ldots p(x_m)}|x_{1A}x_{2A}\ldots x_{mA}\rangle|x_{1B}x_{2B}\ldots x_{mB}\rangle$$

And renormalizing,

$$|\phi'_m\rangle = \frac{|\phi_m\rangle}{\sqrt{\langle\phi_m|\phi_m\rangle}}$$

Then the fidelity

$F(|\psi\rangle^{\otimes m}, |\phi'_m\rangle) \to 1$ as $m \to \infty$.

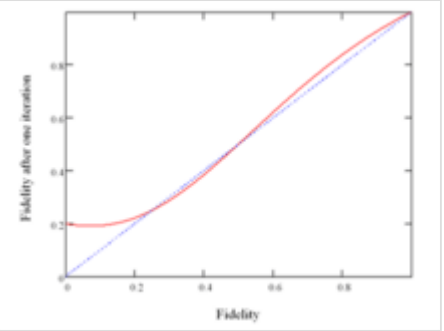
Suppose that Alice and Bob are in possession of m copies of $|\psi\rangle$. Alice can perform a measurement onto the typical set $A_\epsilon^{(n)}$ subset of p_ψ, converting the state $|\psi\rangle^{\otimes m} \to |\phi_m\rangle$ with high fidelity. The theorem of typical sequences then shows us that $1 - \delta$ is the probability that the given sequence is part of the typical set, and may be made arbitrarily close to 1 for sufficiently large m, and therefore the Schmidt coefficients of the renormalized Bell state $|\phi'_m\rangle$ will be at most a factor $1/\sqrt{1-\delta}$ larger. Alice and Bob can now obtain a smaller set of n Bell states by performing LOCC on the state $|\phi'_m\rangle$ with which they can overcome the noise of a quantum channel to communicate successfully.

Mixed states

Many techniques have been developed for doing entanglement distillation for mixed states, giving a lower bounds on the value of the distillable entanglement $D(p)$ for specific classes of states p.

One common method involves Alice not using the noisy channel to transmit source states directly but instead preparing a large number of Bell states, sending half of each Bell pair to Bob. The result from transmission through the noisy channel is to create the mixed entangled state p, so that Alice and Bob end up sharing m copies of p. Alice and Bob then perform entanglement distillation, producing $m \cdot D(p)$

almost perfectly entangled states from the mixed entangled states p by performing local unitary operations and measurements on the shared entangled pairs, coordinating their actions through classical messages, and sacrificing some of the entangled pairs to increase the purity of the remaining ones. Alice can now prepare an $m \cdot D(p)$ qubit state and teleport it to Bob using the $m \cdot D(p)$ Bell pairs which they share with high fidelity. What Alice and Bob have then effectively accomplished is having simulated a noiseless quantum channel using a noisy one, with the aid of local actions and classical communication.



The new fidelity after one iteration of the distillation protocol presented here for mixed states

Let M be a general mixed state of two spin-1/2 particles which could have resulted from the transmission of an initially pure singlet state

$$\psi^- = (\uparrow\downarrow - \downarrow\uparrow)/\sqrt{2}$$

through a noisy channel between Alice and Bob, which will be used to distill some pure entanglement. The fidelity of M

$$F = \langle\psi^-|M|\psi^-\rangle$$

is a convenient expression of its purity relative to a perfect singlet. Suppose that M is already a pure state of two particles $M = |\phi\rangle\langle\phi|$ for some ϕ. The entanglement for ϕ, as already established, is the von Neumann entropy $E(\phi) = S(p_A) = S(p_B)$ where

$$p_A = \mathrm{tr}_B(|\phi\rangle\langle\phi|),$$

and likewise for p_B, represent the reduced density matrices for either particle. The following protocol is then used:[3]

1. Performing a random bilateral rotation on each shared pair, choosing a random SU(2) rotation independently for each pair and applying it locally to both members of the pair transforms the initial general two-spin mixed state M into a rotationally symmetric mixture of the singlet state ψ^- and the three triplet states ψ^+ and $\phi^\pm$:
$$W_F = F \cdot |\psi^-\rangle\langle\psi^-| + \frac{1-F}{3}|\phi^+\rangle\langle\phi^+| + \frac{1-F}{3}|\psi^+\rangle\langle\psi^+| + \frac{1-F}{3}|\phi^-\rangle\langle\phi^-|$$
The Werner state W_F has the same purity F as the initial mixed state M from which it was derived due to the singlet's invariance under bilateral rotations.
2. Each of the two pairs is then acted on by a unilateral rotation, which we can call σ_y, which has the effect of converting them from mainly ψ^- Werner states to mainly ϕ^+ states with a large component $F > \frac{1}{2}$ of ϕ^+ while the components of the other three Bell states are equal.
3. The two impure ϕ^+ states are then acted on by a bilateral XOR, and afterwards the target pair is locally measured along the z axis. The unmeasured source pair is kept if the target pair's spins come out parallel as in the case of both inputs being true ϕ^+ states; and it is discarded otherwise.
4. If the source pair has not been discarded it is converted back to a predominantly ψ^- state by a unilateral σ_y rotation, and made rotationally symmetric by a random bilateral rotation.

Repeating the outlined protocol above will distill Werner states whose purity may be chosen to be arbitrarily high $F_{\text{out}} < 1$ from a collection M of input mixed states of purity $F_{\text{in}} > \frac{1}{2}$ but with a yield tending to zero in the limit $F_{\text{out}} \to 1$. By performing another bilateral XOR operation, this time on a variable number $k(F) \approx \frac{1}{\sqrt{1-F}}$ of source pairs, as opposed to 1, into each target pair prior to measuring it, the yield can be made to approach a positive limit as $F_{\text{out}} \to 1$. This method can then be combined with others to obtain an even higher yield.

Procrustean method

The Procrustean method of entanglement concentration can be used for as little as one partly entangled pair, being more efficient than the Schmidt projection method for entangling less than 5 pairs,[2] and requires Alice and Bob to know the bias (θ) of the n pairs in advance. The method derives its name from Procrustes because it produces a perfectly entangled state by chopping off the extra probability associated with the larger term in the partial entanglement of the pure states:

$$\cos\theta\,|\uparrow_A\rangle \otimes |\downarrow_B\rangle - \sin\theta\,|\downarrow_A\rangle \otimes |\uparrow_B\rangle$$

Assuming a collection of particles for which θ is known as being either less than or greater than $\pi/4$ the Procrustean method may be carried out by keeping all particles which, when passed through a polarization-dependent absorber, or a polarization-dependent-reflector, which absorb or reflect a fraction $\tan^2\theta$ of the more likely outcome, are not absorbed or deflected. Therefore, if Alice possesses particles for which $\theta \neq \pi/4$, she can separate out particles which are more likely to be measured in the up/down basis, and left with particles in maximally mixed state of spin up and spin down. This treatment corresponds to a POVM (positive-operator-valued measurement). To obtain a perfectly entangled state of two particles, Alice informs Bob of the result of her generalized measurement while Bob doesn't measure his particle at all but instead discards his if Alice discards hers.

Stabilizer protocol

The purpose of an $[n, k]$ entanglement distillation protocol is to distill k pure ebits from n noisy ebits where $0 \leq k \leq n$. The yield of such a protocol is k/n. Two parties can then use the noiseless ebits for quantum communication protocols.

The two parties establish a set of shared noisy ebits in the following way. The sender Alice first prepares n Bell states $\left|\Phi^+\right\rangle^{\otimes n}$ locally. She sends the second qubit of each pair over a noisy quantum channel to a receiver Bob. Let $\left|\Phi_n^+\right\rangle$ be the state $\left|\Phi^+\right\rangle^{\otimes n}$ rearranged so that all of Alice's qubits are on the left and all of Bob's qubits are on the right. The noisy quantum channel applies a Pauli error in the error set $\mathcal{E} \subset \Pi^n$ to the set of n qubits sent over the channel. The sender and receiver then share a set of n noisy ebits of the form $(\mathbf{I} \otimes \mathbf{A})\left|\Phi_n^+\right\rangle$ where the identity $\mathbf{I}$ acts on Alice's qubits and $\mathbf{A}$ is some Pauli operator in $\mathcal{E}$ acting on Bob's qubits.

A one-way stabilizer entanglement distillation protocol uses a stabilizer code for the distillation procedure. Suppose the stabilizer $\mathcal{S}$ for an $[n, k]$ quantum error-correcting code has generators $g_1, \ldots, g_{n-k}$. The distillation procedure begins with Alice measuring the $n-k$ generators in $\mathcal{S}$. Let $\{\mathbf{P}_i\}$ be the set of the 2^{n-k} projectors that project onto the 2^{n-k} orthogonal subspaces corresponding to

the generators in $\mathcal{S}$. The measurement projects $\left|\Phi_n^+\right\rangle$ randomly onto one of the i subspaces. Each $\mathbf{P}_i$ commutes with the noisy operator $\mathbf{A}$ on Bob's side so that

$$(\mathbf{P}_i \otimes \mathbf{I})(\mathbf{I} \otimes \mathbf{A})\left|\Phi_n^+\right\rangle = (\mathbf{I} \otimes \mathbf{A})(\mathbf{P}_i \otimes \mathbf{I})\left|\Phi_n^+\right\rangle.$$

The following important *Bell-state matrix identity* holds for an arbitrary matrix $\mathbf{M}$:

$$(\mathbf{M} \otimes \mathbf{I})\left|\Phi_n^+\right\rangle = \left(\mathbf{I} \otimes \mathbf{M}^T\right)\left|\Phi_n^+\right\rangle.$$

Then the above expression is equal to the following:

$$(\mathbf{I} \otimes \mathbf{A})(\mathbf{P}_i \otimes \mathbf{I})\left|\Phi_n^+\right\rangle = (\mathbf{I} \otimes \mathbf{A})\left(\mathbf{P}_i^2 \otimes \mathbf{I}\right)\left|\Phi_n^+\right\rangle = (\mathbf{I} \otimes \mathbf{A})\left(\mathbf{P}_i \otimes \mathbf{P}_i^T\right)\left|\Phi_n^+\right\rangle.$$

Therefore, each of Alice's projectors $\mathbf{P}_i$ projects Bob's qubits onto a subspace $\mathbf{P}_i^T$ corresponding to Alice's projected subspace $\mathbf{P}_i$. Alice restores her qubits to the simultaneous +1-eigenspace of the generators in $\mathcal{S}$. She sends her measurement results to Bob. Bob measures the generators in $\mathcal{S}$. Bob combines his measurements with Alice's to determine a syndrome for the error. He performs a recovery operation on his qubits to reverse the error. He restores his qubits $\mathcal{S}$. Alice and Bob both perform the decoding unitary corresponding to stabilizer $\mathcal{S}$ to convert their k logical ebits to k physical ebits.

Entanglement-assisted stabilizer code

Luo and Devetak provided a straightforward extension of the above protocol (Luo and Devetak 2007). Their method converts an entanglement-assisted stabilizer code into an entanglement-assisted entanglement distillation protocol.

Luo and Devetak form an entanglement distillation protocol that has entanglement assistance from a few noiseless ebits. The crucial assumption for an entanglement-assisted entanglement distillation protocol is that Alice and Bob possess c noiseless ebits in addition to their n noisy ebits. The total state of the noisy and noiseless ebits is

$$\left(\mathbf{I}^A \otimes (\mathbf{A} \otimes \mathbf{I})^B\right)\left|\Phi_{n+c}^+\right\rangle$$

where $\mathbf{I}^A$ is the $2^{n+c} \times 2^{n+c}$ identity matrix acting on Alice's qubits and the noisy Pauli operator $(\mathbf{A} \otimes \mathbf{I})^B$ affects Bob's first n qubits only. Thus the last c ebits are noiseless, and Alice and Bob have to correct for errors on the first n ebits only.

The protocol proceeds exactly as outlined in the previous section. The only difference is that Alice and Bob measure the generators in an entanglement-assisted stabilizer code. Each generator spans over $n + c$ qubits where the last c qubits are noiseless.

We comment on the yield of this entanglement-assisted entanglement distillation protocol. An entanglement-assisted code has $n - k$ generators that each have $n + c$ Pauli entries. These parameters imply that the entanglement distillation protocol produces $k + c$ ebits. But the protocol consumes c initial noiseless ebits as a catalyst for distillation. Therefore, the yield of this protocol is k/n.

Entanglement dilution

The reverse process of entanglement distillation is entanglement dilution, where large copies of the Bell state are converted into less entangled states using LOCC with high fidelity. The aim of the entanglement dilution process, then, is to saturate the inverse ratio of n to m, defined as the distillable entanglement.

Applications

Besides its important application in quantum communication, entanglement purification also plays a crucial role in error correction for quantum computation, because it can significantly increase the quality of logic operations between different qubits. The role of entanglement distillation is discussed briefly for the following applications.

Quantum error correction

Entanglement distillation protocols for mixed states can be used as a type of error-correction for quantum communications channels between two parties Alice and Bob, enabling Alice to reliably send mD(p) qubits of information to Bob, where D(p) is the distillable entanglement of p, the state that results when one half of a Bell pair is sent through the noisy channel ϵ connecting Alice and Bob.

In some cases, entanglement distillation may work when conventional quantum error-correction techniques fail. Entanglement distillation protocols are known which can produce a non-zero rate of transmission D(p) for channels which do not allow the transmission of quantum information due to the property that entanglement distillation protocols allow classical communication between parties as opposed to conventional error-correction which prohibits it.

Quantum cryptography

The concept of correlated measurement outcomes and entanglement is central to quantum key exchange, and therefore the ability to successfully perform entanglement distillation to obtain maximally entangled states is essential for quantum cryptography.

If an entangled pair of particles is shared between two parties, anyone intercepting either particle will alter the overall system, allowing their presence (and the amount of information they have gained) to be determined so long as the particles are in a maximally entangled state. Also, in order to share a secret key string, Alice and Bob must perform the techniques of privacy amplification and information reconciliation to distill a shared secret key string. Information reconciliation is error-correction over a public channel which reconciles errors between the correlated random classical bit strings shared by Alice and Bob while limiting the knowledge that a possible eavesdropper Eve can have about the shared keys. After information reconciliation is used to reconcile possible errors between the shared keys that Alice and Bob possess and limit the possible information Eve could have gained, the technique of privacy amplification is used to distill a smaller subset of bits maximizing Eve's uncertainty about the key.

Quantum teleportation

In quantum teleportation, a sender wishes to transmit an arbitrary quantum state of a particle to a possibly distant receiver. Quantum teleportation is able to achieve faithful transmission of quantum information by substituting classical communication and prior entanglement for a direct quantum channel. Using

teleportation, an arbitrary unknown qubit can be faithfully transmitted via a pair of maximally-entangled qubits shared between sender and receiver, and a 2-bit classical message from the sender to the receiver. Quantum teleportation requires a noiseless quantum channel for sharing perfectly entangled particles, and therefore entanglement distillation satisfies this requirement by providing the noiseless quantum channel and maximally entangled qubits.

See also

- Quantum channel
- Quantum cryptography
- Quantum entanglement
- Quantum state
- Quantum teleportation
- LOCC
- Purification theorem

Notes and references

1. Bennett, Charles H.; DiVincenzo, David P.; Smolin, John A.; Wooters, William K. (1996). "Mixed State Entanglement and Quantum Error Correction". *Phys. Rev. A*. **54** (5): 3824–3851. arXiv:quant-ph/9604024 (https://arxiv.org/abs/quant-ph/9604024). Bibcode:1996PhRvA..54.3824B (https://ui.adsabs.harvard.edu/abs/1996PhRvA..54.3824B). doi:10.1103/physreva.54.3824 (https://doi.org/10.1103%2Fphysreva.54.3824). PMID 9913930 (https://pubmed.ncbi.nlm.nih.gov/9913930). S2CID 3059636 (https://api.semanticscholar.org/CorpusID:3059636).
2. Bennett, Charles H.; Bernstein, Herbert J.; Popescu, Sandu; Schumacher, Benjamin (1996). "Concentrating Partial Entanglement by Local Operations". *Phys. Rev. A*. **53** (4): 2046–2052. arXiv:quant-ph/9511030 (https://arxiv.org/abs/quant-ph/9511030). Bibcode:1996PhRvA..53.2046B (https://ui.adsabs.harvard.edu/abs/1996PhRvA..53.2046B). doi:10.1103/physreva.53.2046 (https://doi.org/10.1103%2Fphysreva.53.2046). PMID 9913106 (https://pubmed.ncbi.nlm.nih.gov/9913106). S2CID 8032709 (https://api.semanticscholar.org/CorpusID:8032709).
3. Bennett, Charles H.; Brassard, Gilles; Popescu, Sandu; Schumacher, Benjamin; Smolin, John A.; Wooters, William K. (1996). "Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels". *Phys. Rev. Lett*. **76** (5): 722–725. arXiv:quant-ph/9511027 (https://arxiv.org/abs/quant-ph/9511027). Bibcode:1996PhRvL..76..722B (https://ui.adsabs.harvard.edu/abs/1996PhRvL..76..722B). doi:10.1103/physrevlett.76.722 (https://doi.org/10.1103%2Fphysrevlett.76.722). PMID 10061534 (https://pubmed.ncbi.nlm.nih.gov/10061534). S2CID 8236531 (https://api.semanticscholar.org/CorpusID:8236531).

- Kwiat, Paul G.; Barraza-Lopez, Salvador; Stefanov, André; Gisin, Nicolas (2001), "Experimental entanglement distillation and 'hidden' non-locality", *Nature*, **409** (6823): 1014–1017, Bibcode:2001Natur.409.1014K (https://ui.adsabs.harvard.edu/abs/2001Natur.409.1014K), doi:10.1038/35059017 (https://doi.org/10.1038%2F35059017), PMID 11234004 (https://pubmed.ncbi.nlm.nih.gov/11234004), S2CID 4430054 (https://api.semanticscholar.org/CorpusID:4430054)

- Yamamoto, Takashi; Koashi, Masato; Özdemir, Şahin Kaya; Imoto, Nobuyuki (2003), "Experimental extraction of an entangled photon pair from two identically decohered pairs", *Nature*, **421** (6921): 343–346, Bibcode:2003Natur.421..343Y (https://ui.adsabs.harvard.edu/abs/2003Natur.421..343Y), doi:10.1038/nature01358 (https://doi.org/10.1038%2Fnature01358), PMID 12540894 (https://pubmed.ncbi.nlm.nih.gov/12540894), S2CID 20824150 (https://api.semanticscholar.org/CorpusID:20824150).
- Pan, Jian-Wei; Gasparoni, Sara; Ursin, Rupert; Weihs, Gregor; Zeilinger, Anton (2003), "Experimental entanglement purification of arbitrary unknown states", *Nature*, **423** (6938): 417–422, Bibcode:2003Natur.423..417P (https://ui.adsabs.harvard.edu/abs/2003Natur.423..417P), doi:10.1038/nature01623 (https://doi.org/10.1038%2Fnature01623), PMID 12761543 (https://pubmed.ncbi.nlm.nih.gov/12761543), S2CID 4393391 (https://api.semanticscholar.org/CorpusID:4393391).
- Pan, Jian-Wei; Simon, Christoph; Brunker, Časlav; Zeilinger, Anton (2001), "Entanglement purification for quantum communication", *Nature*, **410** (6832): 1067–1070, arXiv:quant-ph/0012026 (https://arxiv.org/abs/quant-ph/0012026), Bibcode:2001Natur.410.1067P (https://ui.adsabs.harvard.edu/abs/2001Natur.410.1067P), doi:10.1038/35074041 (https://doi.org/10.1038%2F35074041), PMID 11323664 (https://pubmed.ncbi.nlm.nih.gov/11323664), S2CID 4424450 (https://api.semanticscholar.org/CorpusID:4424450).
- Nielsen, M.A.; Chuang, I.L. (2000), *Quantum Computation and Quantum Information*, Cambridge University Press, ISBN 0521635039
- Bouwmeester, Dirk; Ekert, Artur; Zeilinger, Anton (2000), *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*, Springer, ISBN 3540667784
- Newton, I. (1687), *Principia Mathematica*, vol. 1, Cambridge University Press
- Luo, Zhicheng; Devetak, Igor (2007), "Efficiently implementable codes for quantum key expansion", *Physical Review A*, **75** (1): 010303, arXiv:quant-ph/0608029 (https://arxiv.org/abs/quant-ph/0608029), Bibcode:2007PhRvA..75a0303L (https://ui.adsabs.harvard.edu/abs/2007PhRvA..75a0303L), doi:10.1103/PhysRevA.75.010303 (https://doi.org/10.1103%2FPhysRevA.75.010303), S2CID 119491901 (https://api.semanticscholar.org/CorpusID:119491901)
- Mark M. Wilde, "From Classical to Quantum Shannon Theory", arXiv:1106.1445 (https://arxiv.org/abs/1106.1445).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Entanglement_distillation&oldid=1166432303"

WIKIPEDIA
The Free Encyclopedia

Monogamy of entanglement

In quantum physics, the "**monogamy**" of quantum entanglement refers to the fundamental property that it cannot be freely shared between arbitrarily many parties.

In order for two qubits *A* and *B* to be maximally entangled, they must not be entangled with any third qubit *C* whatsoever. Even if *A* and *B* are not maximally entangled, the degree of entanglement between them constrains the degree to which either can be entangled with *C*. In full generality, for $n \geq 3$ qubits $A_1, \ldots, A_n$, monogamy is characterized by the Coffman–Kundu–Wootters (CKW) inequality, which states that

$$\sum_{k=2}^{n} \tau(\rho_{A_1 A_k}) \leq \tau(\rho_{A_1 (A_2 \ldots A_n)})$$

where $\rho_{A_1 A_k}$ is the density matrix of the substate consisting of qubits A_1 and A_k and τ is the "tangle", a quantification of bipartite entanglement equal to the square of the concurrence.[1][2]

Monogamy, which is closely related to the no-cloning property,[3][4] is purely a feature of quantum correlations, and has no classical analogue. Supposing that two classical random variables *X* and *Y* are correlated, we can copy, or "clone", *X* to create arbitrarily many random variables that all share precisely the same correlation with *Y*. If we let *X* and *Y* be entangled quantum states instead, then *X* cannot be cloned, and this sort of "polygamous" outcome is impossible.

The monogamy of entanglement has broad implications for applications of quantum mechanics ranging from black hole physics to quantum cryptography, where it plays a pivotal role in the security of quantum key distribution.[5]

Proof

The monogamy of bipartite entanglement was established for tripartite systems in terms of concurrence by Coffman, Kundu, and Wootters in 2000.[1] In 2006, Osborne and Verstraete extended this result to the multipartite case, proving the CKW inequality.[2]

Example

For the sake of illustration, consider the three-qubit state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes 3}$ consisting of qubits *A*, *B*, and *C*. Suppose that *A* and *B* form a (maximally entangled) EPR pair. We will show that:

$$|\psi\rangle = |\mathrm{EPR}\rangle_{AB} \otimes |\phi\rangle_C$$

for some valid quantum state $|\phi\rangle_C$. By the definition of entanglement, this implies that *C* must be completely disentangled from *A* and *B*.

When measured in the standard basis, *A* and *B* collapse to the states $|00\rangle$ and $|11\rangle$ with probability $\frac{1}{2}$ each. It follows that:

$$|\psi\rangle = |00\rangle \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle) + |11\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$

for some $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$ such that $|\alpha_0|^2 + |\alpha_1|^2 = |\beta_0|^2 + |\beta_1|^2 = \frac{1}{2}$. We can rewrite the states of *A* and *B* in terms of diagonal basis vectors $|+\rangle$ and $|-\rangle$:

$$|\psi\rangle = \frac{1}{2}(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle) \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle) + \frac{1}{2}(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$
$$= \frac{1}{2}(|++\rangle + |--\rangle) \otimes ((\alpha_0 + \beta_0)|0\rangle + (\alpha_1 + \beta_1)|1\rangle) + \frac{1}{2}(|+-\rangle + |-+\rangle) \otimes ((\alpha_0 - \beta_0)|0\rangle + (\alpha_1 - \beta_1)|1\rangle)$$

Being maximally entangled, *A* and *B* collapse to one of the two states $|++\rangle$ or $|--\rangle$ when measured in the diagonal basis. The probability of observing outcomes $|+-\rangle$ or $|-+\rangle$ is zero. Therefore, according to the equation above, it must be the case that $\alpha_0 - \beta_0 = 0$ and $\alpha_1 - \beta_1 = 0$. It follows immediately that $\alpha_0 = \beta_0$ and $\alpha_1 = \beta_1$. We can rewrite our expression for $|\psi\rangle$ accordingly:

$$|\psi\rangle = (|++\rangle + |--\rangle) \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle)$$
$$= |\mathrm{EPR}\rangle_{AB} \otimes (\sqrt{2}\alpha_0|0\rangle + \sqrt{2}\alpha_1|1\rangle)$$
$$= |\mathrm{EPR}\rangle_{AB} \otimes |\phi\rangle_C$$

This shows that the original state can be written as a product of a pure state in *AB* and a pure state in *C*, which means that the EPR state in qubits *A* and *B* is not entangled with the qubit *C*.

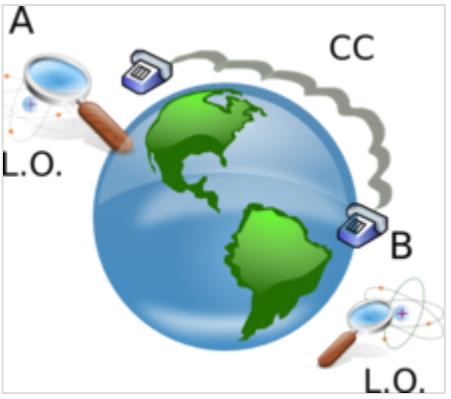
References

1. Coffman, Valerie; Kundu, Joydip; Wootters, William (2000). "Distributed entanglement". *Physical Review A*. **61** (5): 052306. arXiv:quant-ph/9907047 (https://arxiv.org/abs/quant-ph/9907047). Bibcode:2000PhRvA..61e2306C (https://ui.adsabs.harvard.edu/abs/2000PhRvA..61e2306C). doi:10.1103/physreva.61.052306 (https://doi.org/10.1103%2Fphysreva.61.052306). S2CID 1781516 (https://api.semanticscholar.org/CorpusID:1781516).
2. Osborne, Tobias J.; Verstraete, Frank (2006). "General Monogamy Inequality for Bipartite Qubit Entanglement". *Physical Review Letters*. **96** (22): 220503. arXiv:quant-ph/0502176 (https://arxiv.org/abs/quant-ph/0502176). Bibcode:2006PhRvL..96v0503O (https://ui.adsabs.harvard.edu/abs/2006PhRvL..96v0503O). doi:10.1103/PhysRevLett.96.220503 (https://doi.org/10.1103%2FPhysRevLett.96.220503). hdl:1854/LU-8588637 (https://hdl.handle.net/1854%2FLU-8588637). PMID 16803293 (https://pubmed.ncbi.nlm.nih.gov/16803293). S2CID 14366769 (https://api.semanticscholar.org/CorpusID:14366769).
3. Seevnick, Michael (2010). "Monogamy of correlations versus monogamy of entanglement" (https://doi.org/10.1007%2Fs11128-009-0161-6). *Quantum Information Processing*. **9** (2): 273–294. arXiv:0908.1867 (https://arxiv.org/abs/0908.1867). doi:10.1007/s11128-009-0161-6 (https://doi.org/10.1007%2Fs11128-009-0161-6).
4. Pawłowski, Jan Martin (2006). "Quantum dynamics as an analog of conditional probability". *Physical Review A*. **74** (4): 042310. arXiv:quant-ph/0606022 (https://arxiv.org/abs/quant-ph/0606022). Bibcode:2006PhRvA..74d2310L (https://ui.adsabs.harvard.edu/abs/2006PhRvA..74d2310L). doi:10.1103/PhysRevA.74.042310 (https://doi.org/10.1103%2FPhysRevA.74.042310). S2CID 56054135 (https://api.semanticscholar.org/CorpusID:56054135).
5. Leifer, Matthew (2010). "Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations". *Physical Review A*. **82** (3): 032313. arXiv:0907.3778 (https://arxiv.org/abs/0907.3778). Bibcode:2010PhRvA..82c2313P (https://ui.adsabs.harvard.edu/abs/2010PhRvA..82c2313P). doi:10.1103/PhysRevA.82.032313 (https://doi.org/10.1103%2FPhysRevA.82.032313). S2CID 119078270 (https://api.semanticscholar.org/CorpusID:119078270).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Monogamy_of_entanglement&oldid=1228834864"

LOCC

LOCC, or **local operations and classical communication**, is a method in quantum information theory where a local (product) operation is performed on part of the system, and where the result of that operation is "communicated" classically to another part where usually another local operation is performed conditioned on the information received.



LOCC paradigm: the parties are not allowed to exchange particles coherently. Only local operations and classical communication is allowed

Mathematical properties

The formal definition of the set of LOCC operations is complicated due to the fact that later local operations depend in general on all the previous classical communication and due to the unbounded number of communication rounds. For any finite number $r \geq 1$ one can define $\mathbf{LOCC}_r$, the set of LOCC operations that can be achieved with r rounds of classical communication. The set becomes strictly larger whenever r is increased and care has to be taken to define the limit of infinitely many rounds. In particular, the set LOCC is not topologically closed, that is there are quantum operations that can be approximated arbitrarily closely by LOCC but that are not themselves LOCC.[1]

A *one-round* LOCC $\mathbf{LOCC}_1$ is a quantum instrument $\{\mathcal{E}_x\}$, for which the trace-non-increasing completely positive maps (CPMs) $\mathcal{E}_x$ are local for all measurement results x, i.e., $\mathcal{E}_x = \bigotimes_j (\mathcal{E}_x^j)$ and there is one site $j = K$ such that only at K the map $\mathcal{E}_x^K \ \mathcal{E}_x = \bigotimes_{j \neq K} (\mathcal{T}_j^x) \otimes \mathcal{E}_K$ is not trace-preserving. This means that the instrument can be realized by the party at site K applying the (local) instrument $\{\mathcal{E}_x^K\}$ and communicating the classical result x to all other parties, which then each perform (conditioned on x) trace-preserving (deterministic) local quantum operations $\mathcal{T}_x^j$.

Then $\mathbf{LOCC}_r$ are defined recursively as those operations that can be realized by following up an operation $\mathbf{LOCC}_{r-1}$ with a $\mathbf{LOCC}_1$-operation. Here it is allowed that the party which performs the follow-up operations depends on the result of the previous rounds. Moreover, we also allow "coarse-graining", i.e., discarding some of the classical information encoded in the measurement results (of all rounds).

The union of all $\mathbf{LOCC}_r$ operations is denoted by $\mathbf{LOCC}_{\mathbb{N}}$ and contains instruments that can be approximated better and better with more LOCC rounds. Its topological closure $\overline{\mathbf{LOCC}}_{\mathbb{N}}$ contains *all* such operations.

It can be shown that all these sets are different:[1]

$$\mathbf{LOCC}_r \subset \mathbf{LOCC}_{r+1} \subset \mathbf{LOCC}_{\mathbb{N}} \subset \overline{\mathbf{LOCC}}_{\mathbb{N}}$$

The set of all LOCC operations is contained in the set $\mathbf{SEP}$ of all *separable operations*. $\mathbf{SEP}$ contains all operations that can be written using Kraus operators that have all product form, i.e.,

$$\mathcal{E}(\rho) = \sum_l K_1^l \otimes K_2^l \cdots \otimes K_N \rho (K_1^l \otimes K_2^l \cdots \otimes K_N)^\dagger,$$

with $\sum_l K_1^l \otimes K_2^l \cdots \otimes K_N (K_1^l \otimes K_2^l \cdots \otimes K_N)^\dagger = \mathbb{1}$. Not all operations in $\mathbf{SEP}$ are LOCC,

$$\overline{\mathbf{LOCC}}_{\mathbb{N}} \subset \mathbf{SEP},$$

i.e., there are examples that cannot be implemented locally even with infinite rounds of communication.[1]

LOCC are the "free operations" in the resource theories of entanglement: Entanglement cannot be produced from separable states with LOCC and if the local parties in addition to being able to perform all LOCC operations are also furnished with some entangled states, they can realize more operations than with LOCC alone.

Examples

LOCC operations are useful for *state preparation*, *state discrimination*, and *entanglement transformations*.

State preparation

Alice and Bob are given a quantum system in the product state $|00\rangle = |0\rangle_A \otimes |0\rangle_B$. Their task is to produce the separable state $\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$. With local operations alone this cannot be achieved, since they cannot produce the (classical) correlations present in ρ. However, with LOCC (with one round of communication) ρ can be prepared: Alice throws an unbiased coin (that shows heads or tails each with 50% probability) and flips her qubit (to $|1\rangle_A$) if the coin shows "tails", otherwise it is left unchanged. She then sends the result of the coin-flip (classical information) to Bob who also flips his qubit if he receives the message "tails". The resulting state is ρ. In general, *all* separable states (and only these) can be prepared from a product states with LOCC operations alone.[1]

State discrimination

Given two quantum states ψ on a bi- or multipartite Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \ldots \mathcal{H}_Z$, the task is to determine which one of two (or more) possible states ψ_1, ψ_2 it is. As a simple example, consider the two Bell states

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B \right)$$

Let's say the two-qubit system is separated, where the first qubit is given to Alice and the second is given to Bob. Without communication, Alice and Bob cannot distinguish the two states, since for all local measurements all measurement statistics are exactly the same (both states have the same reduced density matrix). E.g., assume that Alice measures the first qubit, and obtains the result 0. Since this result is equally likely to occur (with probability 50%) in each of the two cases, she does not gain any information on which Bell pair she was given and the same holds for Bob if he performs any measurement. But now let Alice send her result to Bob over a classical channel. Now Bob can compare his result to hers and if they are the same he can conclude that the pair given was $|\psi_1\rangle$, since only this allows for a joint measurement outcome $|0\rangle_A \otimes |0\rangle_B$. Thus with LOCC and two measurements these two states can be distinguished perfectly. Note that with global (nonlocal or entangled) measurements, a single measurement (on the joint Hilbert space) is sufficient to distinguish these two (mutually orthogonal) states.

There are quantum states that cannot be distinguished with LOCC operations.[2]

Entanglement transformations

While LOCC cannot *generate* entangled states out of product states, they can be used to transform entangled states into other entangled states. The restriction to LOCC severely limits which transformations are possible.

Entanglement conversion

Nielsen [3] has derived a general condition to determine whether one pure state of a bipartite quantum system may be transformed into another using only LOCC. Full details may be found in the paper referenced earlier, the results are sketched out here.

Consider two particles in a Hilbert space of dimension d with particle states $|\psi\rangle$ and $|\phi\rangle$ with Schmidt decompositions

$$|\psi\rangle = \sum_i \sqrt{\omega_i} |i_A\rangle \otimes |i_B\rangle$$

$$|\phi\rangle = \sum_i \sqrt{\omega'_i} |i'_A\rangle \otimes |i'_B\rangle$$

The $\sqrt{\omega_i}$'s are known as Schmidt coefficients. If they are ordered largest to smallest (i.e., with $\omega_1 > \omega_d$) then $|\psi\rangle$ can only be transformed into $|\phi\rangle$ using only local operations if and only if for all k in the range $1 \leq k \leq d$

$$\sum_{i=1}^{k} \omega_i \leq \sum_{i=1}^{k} \omega'_i$$

In more concise notation:

$$|\psi\rangle \to |\phi\rangle \quad \textbf{iff} \quad \omega \prec \omega'$$

This is a more restrictive condition than that local operations cannot increase entanglement measures. It is quite possible that $|\psi\rangle$ and $|\phi\rangle$ have the same amount of entanglement but converting one into the other is not possible and even that conversion in either direction is impossible because neither set of Schmidt coefficients majorises the other. For large d if all Schmidt coefficients are non-zero then the probability of one set of coefficients majorising the other becomes negligible. Therefore, for large d the probability of any arbitrary state being convertible into another via LOCC becomes negligible.

The operations described so far are deterministic, i.e., they succeed with probability 100%. If one is satisfied by *probabilistic* transformations, many more transformations are possible using LOCC.[4] These operations are called *stochastic* LOCC (SLOCC). In particular for multi-partite states the convertibility under SLOCC is studied to gain a qualitative insight into the entanglement properties of the involved states.[5]

Going beyond LOCC: Catalytic conversion

If entangled states are available as a resource, these together with LOCC allow a much larger class of transformations. This is the case even if these resource states are not consumed in the process (as they are, for example, in quantum teleportation). Thus transformations are called *entanglement catalysis*.[6] In this procedure, the conversion of an initial state to a final state that is impossible with LOCC is made possible by taking a tensor product of the initial state with a "catalyst state" $|c\rangle$ and requiring that this state is still available at the end of the conversion process. I.e., the catalyst state is left unchanged by the conversion and can then be removed, leaving only the desired final state. Consider the states,

$$|\psi\rangle = \sqrt{0.4}|00\rangle + \sqrt{0.4}|11\rangle + \sqrt{0.1}|22\rangle + \sqrt{0.1}|33\rangle$$
$$|\phi\rangle = \sqrt{0.5}|00\rangle + \sqrt{0.25}|11\rangle + \sqrt{0.25}|22\rangle$$
$$|c\rangle = \sqrt{0.6}\ |\uparrow\uparrow\rangle + \sqrt{0.4}\ |\downarrow\downarrow\rangle$$

These states are written in the form of Schmidt decomposition and in a descending order. We compare the sum of the coefficients of $|\psi\rangle$ and $|\phi\rangle$

k	$\|\psi\rangle$	$\|\phi\rangle$
0	0.4	0.5
1	0.8	0.75
2	0.9	1.0
3	1.0	1.0

In the table, red color is put if $\sum_{i=0}^{k} \omega_i > \sum_{i=0}^{k} \omega'_i$, green color is put if $\sum_{i=0}^{k} \omega_i < \sum_{i=0}^{k} \omega'_i$, and white color is remained if $\sum_{i=0}^{k} \omega_i = \sum_{i=0}^{k} \omega'_i$. After building up the table, one can easily to find out whether $|\psi\rangle$ and $|\phi\rangle$ are convertible by looking at the color in the k direction. $|\psi\rangle$ can be converted into $|\phi\rangle$ by LOCC if the color are all green or white, and $|\phi\rangle$ can be converted into $|\psi\rangle$ by LOCC if the color are all red or white. When the table presents both red and green color, the states are not convertible.

Now we consider the product states $|\psi\rangle|c\rangle$ and $|\phi\rangle|c\rangle$：

$$\begin{aligned}|\psi\rangle|c\rangle = & \sqrt{0.24}|00\rangle\ |\uparrow\uparrow\rangle + \sqrt{0.24}|11\rangle\ |\uparrow\uparrow\rangle + \sqrt{0.16}|00\rangle\ |\downarrow\downarrow\rangle + \sqrt{0.16}|11\rangle\ |\downarrow\downarrow\rangle \\ & + \sqrt{0.06}|22\rangle\ |\uparrow\uparrow\rangle + \sqrt{0.06}|33\rangle\ |\uparrow\uparrow\rangle + \sqrt{0.04}|22\rangle\ |\downarrow\downarrow\rangle + \sqrt{0.04}|33\rangle\ |\downarrow\downarrow\rangle \\ |\phi\rangle|c\rangle = & \sqrt{0.30}|00\rangle\ |\uparrow\uparrow\rangle + \sqrt{0.20}|00\rangle\ |\downarrow\downarrow\rangle + \sqrt{0.15}|11\rangle\ |\uparrow\uparrow\rangle + \sqrt{0.15}|22\rangle\ |\uparrow\uparrow\rangle \\ & + \sqrt{0.10}|11\rangle\ |\downarrow\downarrow\rangle + \sqrt{0.10}|22\rangle\ |\downarrow\downarrow\rangle\end{aligned}$$

Similarly, we make up the table:

k	$\|\psi\rangle\|c\rangle$	$\|\phi\rangle\|c\rangle$
0	0.24	0.30
1	0.48	0.50
2	0.64	0.65
3	0.80	0.80
4	0.86	0.90
5	0.92	1.00
6	0.96	1.00
7	1.00	1.00

The color in the k direction are all green or white, therefore, according to the Nielsen's theorem, $|\psi\rangle|c\rangle$ is possible to be converted into $|\phi\rangle|c\rangle$ by the LOCC. The *catalyst* state $|c\rangle$ is taken away after the conversion. Finally we find $|\psi\rangle \xrightarrow{|c\rangle} |\phi\rangle$ by the LOCC.

If correlations between the system and the catalyst are allowed, catalytic transformations between bipartite pure states are characterized via the entanglement entropy.[7] In more detail, a pure state $|\psi\rangle$ can be converted into another pure state $|\phi\rangle$ via catalytic LOCC if and only if

$$S(\psi^A) \geq S(\phi^A),$$

where S is the von Neumann entropy, and ψ^A and ϕ^A are the reduced states of $|\psi\rangle$ and $|\phi\rangle$, respectively. In general, the conversion is not exact, but can be performed with an arbitrary accuracy. The amount of correlations between the system and the catalyst can also be made arbitrarily small.

See also

- Quantum teleportation

References

1. Chitambar, E.; Leung, D.; Mancinska, L.; Ozols, M.; Winter, A. (2012). "Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask)". *Commun. Math. Phys*. **328** (1): 303. arXiv:1210.4583 (https://arxiv.org/abs/1210.4583). Bibcode:2014CMaPh.328..303C (https://ui.adsabs.harvard.edu/abs/2014CMaPh.328..303C). doi:10.1007/s00220-014-1953-

9 (https://doi.org/10.1007%2Fs00220-014-1953-9). S2CID 118478457 (https://api.semanticscholar.org/CorpusID:118478457).
2. Charles H. Bennett; David P. DiVincenzo; Christopher A. Fuchs; Tal Mor; Eric Rains; Peter W. Shor; John A. Smolin; William K. Wootters (1999). "Quantum nonlocality without entanglement". *Phys. Rev. A*. **59** (2): 1070–1091. arXiv:quant-ph/9804053 (https://arxiv.org/abs/quant-ph/9804053). Bibcode:1999PhRvA..59.1070B (https://ui.adsabs.harvard.edu/abs/1999PhRvA..59.1070B). doi:10.1103/PhysRevA.59.1070 (https://doi.org/10.1103%2FPhysRevA.59.1070). S2CID 15282650 (https://api.semanticscholar.org/CorpusID:15282650).
3. M. A. Nielsen (1999). "Conditions for a Class of Entanglement Transformations". *Phys. Rev. Lett*. **83** (2): 436–439. arXiv:quant-ph/9811053 (https://arxiv.org/abs/quant-ph/9811053). Bibcode:1999PhRvL..83..436N (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83..436N). doi:10.1103/PhysRevLett.83.436 (https://doi.org/10.1103%2FPhysRevLett.83.436). S2CID 17928003 (https://api.semanticscholar.org/CorpusID:17928003).
4. Guifré Vidal (2000). "Entanglement Monotones". *J. Mod. Opt*. **47** (2–3): 355. arXiv:quant-ph/9807077 (https://arxiv.org/abs/quant-ph/9807077). Bibcode:2000JMOp...47..355V (https://ui.adsabs.harvard.edu/abs/2000JMOp...47..355V). doi:10.1080/09500340008244048 (https://doi.org/10.1080%2F09500340008244048). S2CID 119347961 (https://api.semanticscholar.org/CorpusID:119347961).
5. G. Gour; N. R. Wallach (2013). "Classification of Multipartite Entanglement of All Finite Dimensionality". *Phys. Rev. Lett*. **111** (6): 060502. arXiv:1304.7259 (https://arxiv.org/abs/1304.7259). Bibcode:2013PhRvL.111f0502G (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111f0502G). doi:10.1103/PhysRevLett.111.060502 (https://doi.org/10.1103%2FPhysRevLett.111.060502). PMID 23971544 (https://pubmed.ncbi.nlm.nih.gov/23971544). S2CID 1570745 (https://api.semanticscholar.org/CorpusID:1570745).
6. D. Jonathan; M. B. Plenio (1999). "Entanglement-assisted local manipulation of pure quantum states". *Phys. Rev. Lett*. **83** (17): 3566–3569. arXiv:quant-ph/9905071 (https://arxiv.org/abs/quant-ph/9905071). Bibcode:1999PhRvL..83.3566J (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83.3566J). doi:10.1103/PhysRevLett.83.3566 (https://doi.org/10.1103%2FPhysRevLett.83.3566). S2CID 392419 (https://api.semanticscholar.org/CorpusID:392419).
7. Kondra, Tulja Varun; Datta, Chandan; Streltsov, Alexander (2021-10-05). "Catalytic Transformations of Pure Entangled States" (https://link.aps.org/doi/10.1103/PhysRevLett.127.150503). *Physical Review Letters*. **127** (15): 150503. arXiv:2102.11136 (https://arxiv.org/abs/2102.11136). Bibcode:2021PhRvL.127o0503K (https://ui.adsabs.harvard.edu/abs/2021PhRvL.127o0503K). doi:10.1103/PhysRevLett.127.150503 (https://doi.org/10.1103%2FPhysRevLett.127.150503). PMID 34678004 (https://pubmed.ncbi.nlm.nih.gov/34678004). S2CID 237532098 (https://api.semanticscholar.org/CorpusID:237532098).

Further reading

- *https://quantiki.org/wiki/locc-operations*
- Nielsen M. A. (1999). "Conditions for a class of entanglement transformations". *Phys. Rev. Lett*. **83** (2): 436–439. arXiv:quant-ph/9811053 (https://arxiv.org/abs/quant-ph/9811053). Bibcode:1999PhRvL..83..436N (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83..436N). doi:10.1103/physrevlett.83.436 (https://doi.org/10.1103%2Fphysrevlett.83.436). S2CID 17928003 (https://api.semanticscholar.org/CorpusID:17928003).

Retrieved from "https://en.wikipedia.org/w/index.php?title=LOCC&oldid=1237425637"

WIKIPEDIA
The Free Encyclopedia

Quantum channel

In quantum information theory, a **quantum channel** is a communication channel which can transmit quantum information, as well as classical information. An example of quantum information is the general dynamics of a qubit. An example of classical information is a text document transmitted over the Internet.

Terminologically, quantum channels are completely positive (CP) trace-preserving maps between spaces of operators. In other words, a quantum channel is just a quantum operation viewed not merely as the reduced dynamics of a system but as a pipeline intended to carry quantum information. (Some authors use the term "quantum operation" to include trace-decreasing maps while reserving "quantum channel" for strictly trace-preserving maps[1])

Memoryless quantum channel

We will assume for the moment that all state spaces of the systems considered, classical or quantum, are finite-dimensional.

The **memoryless** in the section title carries the same meaning as in classical information theory: the output of a channel at a given time depends only upon the corresponding input and not any previous ones.

Schrödinger picture

Consider quantum channels that transmit only quantum information. This is precisely a quantum operation, whose properties we now summarize.

Let H_A and H_B be the state spaces (finite-dimensional Hilbert spaces) of the sending and receiving ends, respectively, of a channel. $L(H_A)$ will denote the family of operators on H_A. In the Schrödinger picture, a purely quantum channel is a map Φ between density matrices acting on H_A and H_B with the following properties:

1. As required by postulates of quantum mechanics, Φ needs to be linear.
2. Since density matrices are positive, Φ must preserve the cone of positive elements. In other words, Φ is a positive map.
3. If an ancilla of arbitrary finite dimension n is coupled to the system, then the induced map $I_n \otimes \Phi$, where I_n is the identity map on the ancilla, must also be positive. Therefore, it is required that $I_n \otimes \Phi$ is positive for all n. Such maps are called completely positive.
4. Density matrices are specified to have trace 1, so Φ has to preserve the trace.

The adjectives **completely positive and trace preserving** used to describe a map are sometimes abbreviated **CPTP**. In the literature, sometimes the fourth property is weakened so that Φ is only required to be not trace-increasing. In this article, it will be assumed that all channels are CPTP.

Heisenberg picture

Density matrices acting on H_A only constitute a proper subset of the operators on H_A and same can be said for system *B*. However, once a linear map $\mathbf{\Phi}$ between the density matrices is specified, a standard linearity argument, together with the finite-dimensional assumption, allow us to extend $\mathbf{\Phi}$ uniquely to the full space of operators. This leads to the adjoint map $\mathbf{\Phi^*}$, which describes the action of $\mathbf{\Phi}$ in the Heisenberg picture:

The spaces of operators $L(H_A)$ and $L(H_B)$ are Hilbert spaces with the Hilbert–Schmidt inner product. Therefore, viewing $\boldsymbol{\Phi : L(H_A) \to L(H_B)}$ as a map between Hilbert spaces, we obtain its adjoint $\mathbf{\Phi}^*$ given by

$$\langle A, \Phi(\rho)\rangle = \langle \Phi^*(A), \rho\rangle.$$

While $\mathbf{\Phi}$ takes states on *A* to those on *B*, $\mathbf{\Phi^*}$ maps observables on system *B* to observables on *A*. This relationship is same as that between the Schrödinger and Heisenberg descriptions of dynamics. The measurement statistics remain unchanged whether the observables are considered fixed while the states undergo operation or vice versa.

It can be directly checked that if $\mathbf{\Phi}$ is assumed to be trace preserving, $\mathbf{\Phi^*}$ is unital, that is,$\boldsymbol{\Phi^*(I) = I}$. Physically speaking, this means that, in the Heisenberg picture, the trivial observable remains trivial after applying the channel.

Classical information

So far we have only defined quantum channel that transmits only quantum information. As stated in the introduction, the input and output of a channel can include classical information as well. To describe this, the formulation given so far needs to be generalized somewhat. A purely quantum channel, in the Heisenberg picture, is a linear map Ψ between spaces of operators:

$$\boldsymbol{\Psi : L(H_B) \to L(H_A)}$$

that is unital and completely positive (**CP**). The operator spaces can be viewed as finite-dimensional C*-algebras. Therefore, we can say a channel is a unital CP map between C*-algebras:

$$\boldsymbol{\Psi : \mathcal{B} \to \mathcal{A}}.$$

Classical information can then be included in this formulation. The observables of a classical system can be assumed to be a commutative C*-algebra, i.e. the space of continuous functions $\boldsymbol{C(X)}$ on some set $\boldsymbol{X}$. We assume $\boldsymbol{X}$ is finite so $\boldsymbol{C(X)}$ can be identified with the *n*-dimensional Euclidean space $\mathbb{R}^{\boldsymbol{n}}$ with entry-wise multiplication.

Therefore, in the Heisenberg picture, if the classical information is part of, say, the input, we would define $\boldsymbol{\mathcal{B}}$ to include the relevant classical observables. An example of this would be a channel

$$\boldsymbol{\Psi : L(H_B) \otimes C(X) \to L(H_A)}.$$

Notice $\boldsymbol{L(H_B) \otimes C(X)}$ is still a C*-algebra. An element $\boldsymbol{a}$ of a C*-algebra $\boldsymbol{\mathcal{A}}$ is called positive if $\boldsymbol{a = x^* x}$ for some $\boldsymbol{x}$. Positivity of a map is defined accordingly. This characterization is not universally accepted; the quantum instrument is sometimes given as the generalized mathematical framework for

conveying both quantum and classical information. In axiomatizations of quantum mechanics, the classical information is carried in a Frobenius algebra or Frobenius category.

Examples

Time evolution

For a purely quantum system, the time evolution, at certain time *t*, is given by

$$\rho \to U\rho\, U^*,$$

where $U = e^{-iHt/\hbar}$ and *H* is the Hamiltonian and *t* is the time. Clearly this gives a CPTP map in the Schrödinger picture and is therefore a channel. The dual map in the Heisenberg picture is

$$A \to U^* A U.$$

Restriction

Consider a composite quantum system with state space $H_A \otimes H_B$. For a state

$$\rho \in H_A \otimes H_B,$$

the reduced state of ρ on system *A*, ρ^A, is obtained by taking the partial trace of ρ with respect to the *B* system:

$$\rho^A = \mathrm{Tr}_B\ \rho.$$

The partial trace operation is a CPTP map, therefore a quantum channel in the Schrödinger picture. In the Heisenberg picture, the dual map of this channel is

$$A \to A \otimes I_B,$$

where *A* is an observable of system *A*.

Observable

An observable associates a numerical value $f_i \in \mathbb{C}$ to a quantum mechanical *effect* F_i. F_i's are assumed to be positive operators acting on appropriate state space and $\sum_i F_i = I$. (Such a collection is called a POVM.) In the Heisenberg picture, the corresponding *observable map* Ψ maps a classical observable

$$f = \begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} \in C(X)$$

to the quantum mechanical one

$$\Psi(f) = \sum_i f_i F_i.$$

In other words, one integrates f against the POVM to obtain the quantum mechanical observable. It can be easily checked that Ψ is CP and unital.

The corresponding Schrödinger map Ψ^* takes density matrices to classical states:

$$\Psi(\rho) = \begin{bmatrix} \langle F_1, \rho \rangle \\ \vdots \\ \langle F_n, \rho \rangle \end{bmatrix},$$

where the inner product is the Hilbert–Schmidt inner product. Furthermore, viewing states as normalized functionals, and invoking the Riesz representation theorem, we can put

$$\Psi(\rho) = \begin{bmatrix} \rho(F_1) \\ \vdots \\ \rho(F_n) \end{bmatrix}.$$

Instrument

The observable map, in the Schrödinger picture, has a purely classical output algebra and therefore only describes measurement statistics. To take the state change into account as well, we define what is called a quantum instrument. Let $\{F_1, \ldots, F_n\}$ be the effects (POVM) associated to an observable. In the Schrödinger picture, an instrument is a map Φ with pure quantum input $\rho \in L(H)$ and with output space $C(X) \otimes L(H)$:

$$\Phi(\rho) = \begin{bmatrix} \rho(F_1) \cdot F_1 \\ \vdots \\ \rho(F_n) \cdot F_n \end{bmatrix}.$$

Let

$$f = \begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} \in C(X).$$

The dual map in the Heisenberg picture is

$$\Psi(f \otimes A) = \begin{bmatrix} f_1 \Psi_1(A) \\ \vdots \\ f_n \Psi_n(A) \end{bmatrix}$$

where Ψ_i is defined in the following way: Factor $F_i = M_i^2$ (this can always be done since elements of a POVM are positive) then $\Psi_i(A) = M_i A M_i$. We see that Ψ is CP and unital.

Notice that $\Psi(f \otimes I)$ gives precisely the observable map. The map

$$\tilde{\Psi}(A) = \sum_i \Psi_i(A) = \sum_i M_i A M_i$$

describes the overall state change.

Measure-and-prepare channel

Suppose two parties *A* and *B* wish to communicate in the following manner: *A* performs the measurement of an observable and communicates the measurement outcome to *B* classically. According to the message he receives, *B* prepares his (quantum) system in a specific state. In the Schrödinger picture, the first part of the channel Φ_1 simply consists of *A* making a measurement, i.e. it is the observable map:

$$\Phi_1(\rho) = \begin{bmatrix} \rho(F_1) \\ \vdots \\ \rho(F_n) \end{bmatrix}.$$

If, in the event of the *i*-th measurement outcome, *B* prepares his system in state R_i, the second part of the channel Φ_2 takes the above classical state to the density matrix

$$\Phi_2\left(\begin{bmatrix} \rho(F_1) \\ \vdots \\ \rho(F_n) \end{bmatrix}\right) = \sum_i \rho(F_i) R_i.$$

The total operation is the composition

$$\Phi(\rho) = \Phi_2 \circ \Phi_1(\rho) = \sum_i \rho(F_i) R_i.$$

Channels of this form are called *measure-and-prepare* or in Holevo form.

In the Heisenberg picture, the dual map $\Phi^* = \Phi_1^* \circ \Phi_2^*$ is defined by

$$\Phi^*(A) = \sum_i R_i(A) F_i.$$

A measure-and-prepare channel can not be the identity map. This is precisely the statement of the no teleportation theorem, which says classical teleportation (not to be confused with entanglement-assisted teleportation) is impossible. In other words, a quantum state can not be measured reliably.

In the channel-state duality, a channel is measure-and-prepare if and only if the corresponding state is separable. Actually, all the states that result from the partial action of a measure-and-prepare channel are separable, and for this reason measure-and-prepare channels are also known as entanglement-breaking channels.

Pure channel

Consider the case of a purely quantum channel Ψ in the Heisenberg picture. With the assumption that everything is finite-dimensional, Ψ is a unital CP map between spaces of matrices

$$\Psi : \mathbb{C}^{n\times n} \to \mathbb{C}^{m\times m}.$$

By Choi's theorem on completely positive maps, Ψ must take the form

$$\Psi(A) = \sum_{i=1}^{N} K_i A K_i^*$$

where $N \leq nm$. The matrices K_i are called **Kraus operators** of Ψ (after the German physicist Karl Kraus, who introduced them). The minimum number of Kraus operators is called the Kraus rank of Ψ. A channel with Kraus rank 1 is called **pure**. The time evolution is one example of a pure channel. This terminology again comes from the channel-state duality. A channel is pure if and only if its dual state is a pure state.

Teleportation

In quantum teleportation, a sender wishes to transmit an arbitrary quantum state of a particle to a possibly distant receiver. Consequently, the teleportation process is a quantum channel. The apparatus for the process itself requires a quantum channel for the transmission of one particle of an entangled-state to the receiver. Teleportation occurs by a joint measurement of the sent particle and the remaining entangled particle. This measurement results in classical information which must be sent to the receiver to complete the teleportation. Importantly, the classical information can be sent after the quantum channel has ceased to exist.

In the experimental setting

Experimentally, a simple implementation of a quantum channel is fiber optic (or free-space for that matter) transmission of single photons. Single photons can be transmitted up to 100 km in standard fiber optics before losses dominate. The photon's time-of-arrival (*time-bin entanglement*) or polarization are used as a basis to encode quantum information for purposes such as quantum cryptography. The channel is capable of transmitting not only basis states (e.g. $|0\rangle$, $|1\rangle$) but also superpositions of them (e.g. $|0\rangle + |1\rangle$). The coherence of the state is maintained during transmission through the channel. Contrast this with the transmission of electrical pulses through wires (a classical channel), where only classical information (e.g. 0s and 1s) can be sent.

Channel capacity

The cb-norm of a channel

Before giving the definition of channel capacity, the preliminary notion of the **norm of complete boundedness**, or **cb-norm** of a channel needs to be discussed. When considering the capacity of a channel Φ, we need to compare it with an "ideal channel" Λ . For instance, when the input and output algebras are identical, we can choose Λ to be the identity map. Such a comparison requires a metric between channels. Since a channel can be viewed as a linear operator, it is tempting to use the natural operator norm. In other words, the closeness of Φ to the ideal channel Λ can be defined by

$$\|\Phi - \Lambda\| = \sup\{\|(\Phi - \Lambda)(A)\| \mid \|A\| \leq 1\}.$$

However, the operator norm may increase when we tensor Φ with the identity map on some ancilla.

To make the operator norm even a more undesirable candidate, the quantity

$$\|\Phi \otimes I_n\|$$

may increase without bound as $n \to \infty$. The solution is to introduce, for any linear map Φ between C*-algebras, the cb-norm

$$\|\Phi\|_{cb} = \sup_n \|\Phi \otimes I_n\|.$$

Definition of channel capacity

The mathematical model of a channel used here is same as the classical one.

Let $\Psi : \mathcal{B}_1 \to \mathcal{A}_1$ be a channel in the Heisenberg picture and $\Psi_{id} : \mathcal{B}_2 \to \mathcal{A}_2$ be a chosen ideal channel. To make the comparison possible, one needs to encode and decode Φ via appropriate devices, i.e. we consider the composition

$$\hat{\Psi} = D \circ \Phi \circ E : \mathcal{B}_2 \to \mathcal{A}_2$$

where *E* is an encoder and *D* is a decoder. In this context, *E* and *D* are unital CP maps with appropriate domains. The quantity of interest is the *best case scenario*:

$$\Delta(\hat{\Psi}, \Psi_{id}) = \inf_{E,D} \|\hat{\Psi} - \Psi_{id}\|_{cb}$$

with the infimum being taken over all possible encoders and decoders.

To transmit words of length *n*, the ideal channel is to be applied *n* times, so we consider the tensor power

$$\Psi_{id}^{\otimes n} = \Psi_{id} \otimes \cdots \otimes \Psi_{id}.$$

The $\otimes$ operation describes *n* inputs undergoing the operation Ψ_{id} independently and is the quantum mechanical counterpart of concatenation. Similarly, *m invocations of the channel* corresponds to $\hat{\Psi}^{\otimes m}$.

The quantity

$$\Delta(\hat{\Psi}^{\otimes m}, \Psi_{id}^{\otimes n})$$

is therefore a measure of the ability of the channel to transmit words of length *n* faithfully by being invoked *m* times.

This leads to the following definition:

A non-negative real number *r* is an **achievable rate of Ψ with respect to Ψ_{id}** if

For all sequences $\{n_\alpha\}, \{m_\alpha\} \subset \mathbb{N}$ where $m_\alpha \to \infty$ and $\limsup_\alpha (n_\alpha / m_\alpha) < r$, we have

$$\lim_\alpha \Delta(\hat{\Psi}^{\otimes m_\alpha}, \Psi_{id}^{\otimes n_\alpha}) = 0.$$

A sequence $\{n_\alpha\}$ can be viewed as representing a message consisting of possibly infinite number of words. The limit supremum condition in the definition says that, in the limit, faithful transmission can be achieved by invoking the channel no more than *r* times the length of a word. One can also say that *r* is the number of letters per invocation of the channel that can be sent without error.

The **channel capacity of Ψ with respect to Ψ_{id}**, denoted by $C(\Psi, \Psi_{id})$ is the supremum of all achievable rates.

From the definition, it is vacuously true that 0 is an achievable rate for any channel.

Important examples

As stated before, for a system with observable algebra $\mathcal{B}$, the ideal channel Ψ_{id} is by definition the identity map $I_{\mathcal{B}}$. Thus for a purely *n* dimensional quantum system, the ideal channel is the identity map on the space of *n* × *n* matrices $\mathbb{C}^{n\times n}$. As a slight abuse of notation, this ideal quantum channel will be also denoted by $\mathbb{C}^{n\times n}$. Similarly, a classical system with output algebra $\mathbb{C}^m$ will have an ideal channel denoted by the same symbol. We can now state some fundamental channel capacities.

The channel capacity of the classical ideal channel $\mathbb{C}^m$ with respect to a quantum ideal channel $\mathbb{C}^{n\times n}$ is

$$C(\mathbb{C}^m, \mathbb{C}^{n\times n}) = 0.$$

This is equivalent to the no-teleportation theorem: it is impossible to transmit quantum information via a classical channel.

Moreover, the following equalities hold:

$$C(\mathbb{C}^m, \mathbb{C}^n) = C(\mathbb{C}^{m\times m}, \mathbb{C}^{n\times n}) = C(\mathbb{C}^{m\times m}, \mathbb{C}^n) = \frac{\log n}{\log m}.$$

The above says, for instance, an ideal quantum channel is no more efficient at transmitting classical information than an ideal classical channel. When *n* = *m*, the best one can achieve is *one bit per qubit*.

It is relevant to note here that both of the above bounds on capacities can be broken, with the aid of entanglement. The entanglement-assisted teleportation scheme allows one to transmit quantum information using a classical channel. Superdense coding. achieves *two bit per qubit*. These results indicate the significant role played by entanglement in quantum communication.

Classical and quantum channel capacities

Using the same notation as the previous subsection, the **classical capacity** of a channel Ψ is

$$C(\Psi, \mathbb{C}^2),$$

that is, it is the capacity of Ψ with respect to the ideal channel on the classical one-bit system $\mathbb{C}^2$.

Similarly the **quantum capacity** of Ψ is

$$C(\Psi, \mathbb{C}^{2\times 2}),$$

where the reference system is now the one qubit system $\mathbb{C}^{2\times 2}$.

Channel fidelity

Another measure of how well a quantum channel preserves information is called **channel fidelity**, and it arises from fidelity of quantum states.

Bistochastic quantum channel

A bistochastic quantum channel is a quantum channel $\Phi(\rho)$ which is unital,[2] i.e. $\Phi(I) = I$.

See also

- No-communication theorem
- Amplitude damping channel
- Quantum depolarizing channel

References

1. Weedbrook, Christian; Pirandola, Stefano; García-Patrón, Raúl; Cerf, Nicolas J.; Ralph, Timothy C.; Shapiro, Jeffrey H.; Lloyd, Seth (2012). "Gaussian quantum information". *Reviews of Modern Physics*. **84** (2): 621–669. arXiv:1110.3234 (https://arxiv.org/abs/1110.3234). Bibcode:2012RvMP...84..621W (https://ui.adsabs.harvard.edu/abs/2012RvMP...84..621W). doi:10.1103/RevModPhys.84.621 (https://doi.org/10.1103%2FRevModPhys.84.621). S2CID 119250535 (https://api.semanticscholar.org/CorpusID:119250535).
2. John A. Holbrook, David W. Kribs, and Raymond Laflamme. "Noiseless Subsystems and the Structure of the Commutant in Quantum Error Correction." *Quantum Information Processing*. Volume 2, Number 5, p. 381-419. Oct 2003.

- M. Keyl and R. F. Werner, *How to Correct Small Quantum Errors*, Lecture Notes in Physics Volume 611, Springer, 2002.
- Wilde, Mark M. (2017), *Quantum Information Theory*, Cambridge University Press, arXiv:1106.1445 (https://arxiv.org/abs/1106.1445), Bibcode:2011arXiv1106.1445W (https://ui.adsabs.harvard.edu/abs/2011arXiv1106.1445W), doi:10.1017/9781316809976.001 (https://doi.org/10.1017%2F9781316809976.001), S2CID 2515538 (https://api.semanticscholar.org/CorpusID:2515538).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_channel&oldid=1243698230"

WIKIPEDIA
The Free Encyclopedia

Quantum network

Quantum networks form an important element of quantum computing and quantum communication systems. Quantum networks facilitate the transmission of information in the form of quantum bits, also called qubits, between physically separated quantum processors. A quantum processor is a machine able to perform quantum circuits on a certain number of qubits. Quantum networks work in a similar way to classical networks. The main difference is that quantum networking, like quantum computing, is better at solving certain problems, such as modeling quantum systems.

Basics

Quantum networks for computation

Networked quantum computing or distributed quantum computing[1][2] works by linking multiple quantum processors through a quantum network by sending qubits in between them. Doing this creates a quantum computing cluster and therefore creates more computing potential. Less powerful computers can be linked in this way to create one more powerful processor. This is analogous to connecting several classical computers to form a computer cluster in classical computing. Like classical computing, this system is scalable by adding more and more quantum computers to the network. Currently quantum processors are only separated by short distances.

Quantum networks for communication

In the realm of quantum communication, one wants to send qubits from one quantum processor to another over long distances.[3] This way, local quantum networks can be intra connected into a quantum internet. A quantum internet[1] supports many applications, which derive their power from the fact that by creating quantum entangled qubits, information can be transmitted between the remote quantum processors. Most applications of a quantum internet require only very modest quantum processors. For most quantum internet protocols, such as quantum key distribution in quantum cryptography, it is sufficient if these processors are capable of preparing and measuring only a single qubit at a time. This is in contrast to quantum computing where interesting applications can be realized only if the (combined) quantum processors can easily simulate more qubits than a classical computer (around 60[4]). Quantum internet applications require only small quantum processors, often just a single qubit, because quantum entanglement can already be realized between just two qubits. A simulation of an entangled quantum system on a classical computer cannot simultaneously provide the same security and speed.

Overview of the elements of a quantum network

The basic structure of a quantum network and more generally a quantum internet is analogous to a classical network. First, we have end nodes on which applications are ultimately run. These end nodes are quantum processors of at least one qubit. Some applications of a quantum internet require quantum processors of several qubits as well as a quantum memory at the end nodes.

Second, to transport qubits from one node to another, we need communication lines. For the purpose of quantum communication, standard telecom fibers can be used. For networked quantum computing, in which quantum processors are linked at short distances, different wavelengths are chosen depending on the exact hardware platform of the quantum processor.

Third, to make maximum use of communication infrastructure, one requires optical switches capable of delivering qubits to the intended quantum processor. These switches need to preserve quantum coherence, which makes them more challenging to realize than standard optical switches.

Finally, one requires a quantum repeater to transport qubits over long distances. Repeaters appear in between end nodes.[5] Since qubits cannot be copied (No-cloning theorem), classical signal amplification is not possible. By necessity, a quantum repeater works in a fundamentally different way than a classical repeater.

Elements of a quantum network

End nodes: quantum processors

End nodes can both receive and emit information.[5] Telecommunication lasers and parametric down-conversion combined with photodetectors can be used for quantum key distribution. In this case, the end nodes can in many cases be very simple devices consisting only of beamsplitters and photodetectors.

However, for many protocols more sophisticated end nodes are desirable. These systems provide advanced processing capabilities and can also be used as quantum repeaters. Their chief advantage is that they can store and retransmit quantum information without disrupting the underlying quantum state. The quantum state being stored can either be the relative spin of an electron in a magnetic field or the energy state of an electron.[5] They can also perform quantum logic gates.

One way of realizing such end nodes is by using color centers in diamond, such as the nitrogen-vacancy center. This system forms a small quantum processor featuring several qubits. NV centers can be utilized at room temperatures.[5] Small scale quantum algorithms and quantum error correction[6] has already been demonstrated in this system, as well as the ability to entangle two[7] and three[8] quantum processors, and perform deterministic quantum teleportation.[9]

Another possible platform are quantum processors based on ion traps, which utilize radio-frequency magnetic fields and lasers.[5] In a multispecies trapped-ion node network, photons entangled with a parent atom are used to entangle different nodes.[10] Also, cavity quantum electrodynamics (Cavity QED) is one possible method of doing this. In Cavity QED, photonic quantum states can be transferred to and from atomic quantum states stored in single atoms contained in optical cavities. This allows for the transfer of quantum states between single atoms using optical fiber in addition to the creation of remote entanglement between distant atoms.[5][11][12]

Communication lines: physical layer

Over long distances, the primary method of operating quantum networks is to use optical networks and photon-based qubits. This is due to optical networks having a reduced chance of decoherence. Optical networks have the advantage of being able to re-use existing optical fiber. Alternately, free space networks can be implemented that transmit quantum information through the atmosphere or through a vacuum.[13]

Fiber optic networks

Optical networks using existing telecommunication fiber can be implemented using hardware similar to existing telecommunication equipment. This fiber can be either single-mode or multi-mode, with single-mode allowing for more precise communication.[5] At the sender, a *single photon* source can be created by heavily attenuating a standard telecommunication laser such that the mean number of photons per pulse is less than 1. For receiving, an avalanche photodetector can be used. Various methods of phase or polarization control can be used such as interferometers and beam splitters. In the case of entanglement based protocols, entangled photons can be generated through spontaneous parametric down-conversion. In both cases, the telecom fiber can be multiplexed to send non-quantum timing and control signals.

In 2020 a team of researchers affiliated with several institutions in China has succeeded in sending entangled quantum memories over a 50-kilometer coiled fiber cable.[14]

Free space networks

Free space quantum networks operate similar to fiber optic networks but rely on line of sight between the communicating parties instead of using a fiber optic connection. Free space networks can typically support higher transmission rates than fiber optic networks and do not have to account for polarization scrambling caused by optical fiber.[15] However, over long distances, free space communication is subject to an increased chance of environmental disturbance on the photons.[5]

Free space communication is also possible from a satellite to the ground. A quantum satellite capable of entanglement distribution over a distance of 1,203 km[16] has been demonstrated. The experimental exchange of single photons from a global navigation satellite system at a slant distance of 20,000 km has also been reported.[17] These satellites can play an important role in linking smaller ground-based networks over larger distances.

Repeaters

Long-distance communication is hindered by the effects of signal loss and decoherence inherent to most transport mediums such as optical fiber. In classical communication, amplifiers can be used to boost the signal during transmission, but in a quantum network amplifiers cannot be used since qubits cannot be copied – known as the no-cloning theorem. That is, to implement an amplifier, the complete state of the flying qubit would need to be determined, something which is both unwanted and impossible.

Trusted repeaters

An intermediary step which allows the testing of communication infrastructure are trusted repeaters. Importantly, a trusted repeater cannot be used to transmit qubits over long distances. Instead, a trusted repeater can only be used to perform quantum key distribution with the additional assumption that the repeater is trusted. Consider two end nodes A and B, and a trusted repeater R in the middle. A and R now perform quantum key distribution to generate a key k_{AR}. Similarly, R and B run quantum key distribution to generate a key k_{RB}. A and B can now obtain a key k_{AB} between themselves as follows: A sends k_{AB} to R encrypted with the key k_{AR}. R decrypts to obtain k_{AB}. R then re-encrypts k_{AB} using the key k_{RB} and sends it to B. B decrypts to obtain k_{AB}. A and B now share the key k_{AB}. The key is secure from an outside eavesdropper, but clearly the repeater R also knows k_{AB}. This means that any subsequent communication between A and B does not provide end to end security, but is only secure as long as A and B trust the repeater R.

Quantum repeaters

A true quantum repeater allows the end to end generation of quantum entanglement, and thus – by using quantum teleportation – the end to end transmission of qubits. In quantum key distribution protocols one can test for such entanglement. This means that when making encryption keys, the sender and receiver are secure even if they do not trust the quantum repeater. Any other application of a quantum internet also requires the end to end transmission of qubits, and thus a quantum repeater.

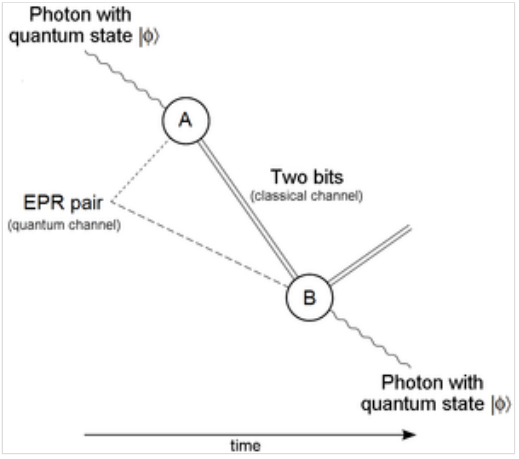


Diagram for quantum teleportation of a photon

Quantum repeaters allow entanglement and can be established at distant nodes without physically sending an entangled qubit the entire distance.[18]

In this case, the quantum network consists of many short distance links of perhaps tens or hundreds of kilometers. In the simplest case of a single repeater, two pairs of entangled qubits are established: $|A\rangle$ and $|R_a\rangle$ located at the sender and the repeater, and a second pair $|R_b\rangle$ and $|B\rangle$ located at the repeater and the receiver. These initial entangled qubits can be easily created, for example through parametric down conversion, with one qubit physically transmitted to an adjacent node. At this point, the repeater can perform a Bell measurement on the qubits $|R_a\rangle$ and $|R_b\rangle$ thus teleporting the quantum state of $|R_a\rangle$ onto $|B\rangle$. This has the effect of "swapping" the entanglement such that $|A\rangle$ and $|B\rangle$ are now entangled at a distance twice that of the initial entangled pairs. It can be seen that a network of such repeaters can be used linearly or in a hierarchical fashion to establish entanglement over great distances.[19][20]

Hardware platforms suitable as end nodes above can also function as quantum repeaters. However, there are also hardware platforms specific only[21] to the task of acting as a repeater, without the capabilities of performing quantum gates.

Error correction

Error correction can be used in quantum repeaters. Due to technological limitations, however, the applicability is limited to very short distances as quantum error correction schemes capable of protecting qubits over long distances would require an extremely large amount of qubits and hence extremely large quantum computers.

Errors in communication can be broadly classified into two types: Loss errors (due to optical fiber/environment) and operation errors (such as depolarization, dephasing etc.). While redundancy can be used to detect and correct classical errors, redundant qubits cannot be created due to the no-cloning theorem. As a result, other types of error correction must be introduced such as the Shor code or one of a number of more general and efficient codes. All of these codes work by distributing the quantum information across multiple entangled qubits so that operation errors as well as loss errors can be corrected.[22]

In addition to quantum error correction, classical error correction can be employed by quantum networks in special cases such as quantum key distribution. In these cases, the goal of the quantum communication is to securely transmit a string of classical bits. Traditional error correction codes such as Hamming codes can be applied to the bit string before encoding and transmission on the quantum network.

Entanglement purification

Quantum decoherence can occur when one qubit from a maximally entangled bell state is transmitted across a quantum network. Entanglement purification allows for the creation of nearly maximally entangled qubits from a large number of arbitrary weakly entangled qubits, and thus provides additional protection against errors. Entanglement purification (also known as Entanglement distillation) has already been demonstrated in Nitrogen-vacancy centers in diamond.[23]

Applications

A quantum internet supports numerous applications, enabled by quantum entanglement. In general, quantum entanglement is well suited for tasks that require coordination, synchronization or privacy.

Examples of such applications include quantum key distribution,[24][25] clock stabilization,[26] protocols for distributed system problems such as leader election or Byzantine agreement,[5] extending the baseline of telescopes,[27][28] as well as position verification,[29][30] secure identification and two-party cryptography in the noisy-storage model. A quantum internet also enables secure access to a quantum computer[31] in the cloud. Specifically, a quantum internet enables very simple quantum devices to connect to a remote quantum computer in such a way that computations can be performed there without the quantum computer finding out what this computation actually is (the input and output quantum states can not be measured without destroying the computation, but the circuit composition used for the calculation will be known).

Secure communications

When it comes to communicating in any form the largest issue has always been keeping these communications private.[32] Quantum networks would allow for information to be created, stored and transmitted, potentially achieving "a level of privacy, security and computational clout that is impossible to achieve with today's Internet."[33]

By applying a quantum operator that the user selects to a system of information the information can then be sent to the receiver without a chance of an eavesdropper being able to accurately be able to record the sent information without either the sender or receiver knowing. Unlike classical information that is transmitted in bits and assigned either a 0 or 1 value, the quantum information used in quantum networks uses quantum bits (qubits), which can have both 0 and 1 value at the same time, being in a state of superposition.[33][34] This works because if a listener tries to listen in then they will change the information in an unintended way by listening, thereby tipping their hand to the people on whom they are attacking.

Secondly, without the proper quantum operator to decode the information they will corrupt the sent information without being able to use it themselves. Furthermore, qubits can be encoded in a variety of materials, including in the polarization of photons or the spin states of electrons.[33]

Current status

Quantum internet

As of May 20,2024, a quantum Internet mile stone takes place out of the lab and into the cities. The feat is a key step towards a future quantum Internet. At present, there is continuing research on network connecting quantum processors, or quantum repeaters deployed outside a lab. Teams in the Netherlands, China and United States collaborated on the new feat.

One example of a prototype quantum communication network is the eight-user city-scale quantum network described in a paper published in September 2020. The network located in Bristol used already deployed fibre-infrastructure and worked without active switching or trusted nodes.[35][36]

In 2022, Researchers at the University of Science and Technology of China and Jinan Institute of Quantum Technology demonstrated quantum entanglement between two memory devices located at 12.5 km apart from each other within an urban environment.[37]

In the same year, Physicist at the Delft University of Technology in Netherlands has taken a significant step toward the network of the future by using a technique called quantum teleportation that sends data to three physical locations which was previously only possible with two locations.[38]

In 2024, researchers in the U.K and Germany achieved a first by producing, storing, and retrieving quantum information. This milestone involved interfacing a quantum dot light source and a quantum memory system, paving the way for practical applications despite challenges like quantum information loss over long distances.[39]

Quantum networks for computation

In 2021, researchers at the Max Planck Institute of Quantum Optics in Germany reported a first prototype of quantum logic gates for distributed quantum computers.[40][41]

Experimental quantum modems

A research team at the Max-Planck-Institute of Quantum Optics in Garching, Germany is finding success in transporting quantum data from flying and stable qubits via infrared spectrum matching. This requires a sophisticated, super-cooled yttrium silicate crystal to sandwich erbium in a mirrored environment to achieve resonance matching of infrared wavelengths found in fiber optic networks. The team successfully demonstrated the device works without data loss.[42]

Mobile quantum networks

In 2021, researchers in China reported the successful transmission of entangled photons between drones, used as nodes for the development of mobile quantum networks or flexible network extensions. This could be the first work in which entangled particles were sent between two moving devices.[43][44]

Quantum key distribution networks

Several test networks have been deployed that are tailored to the task of quantum key distribution either at short distances (but connecting many users), or over larger distances by relying on trusted repeaters. These networks do not yet allow for the end to end transmission of qubits or the end to end creation of entanglement between far away nodes.

Major quantum network projects and QKD protocols implemented

Quantum network	Start	BB84	BBM92	E91	DPS	COW
DARPA Quantum Network	2001	Yes	No	No	No	No
SECOCQ QKD network in Vienna	2003	Yes	Yes	No	No	Yes
Tokyo QKD network	2009	Yes	Yes	No	Yes	No
Hierarchical network in Wuhu, China	2009	Yes	No	No	No	No
Geneva area network (SwissQuantum)	2010	Yes	No	No	No	Yes

DARPA Quantum Network

Starting in the early 2000s, DARPA began sponsorship of a quantum network development project with the aim of implementing secure communication. The DARPA Quantum Network became operational within the BBN Technologies laboratory in late 2003 and was expanded further in 2004 to include nodes at Harvard and Boston Universities. The network consists of multiple physical layers including fiber optics supporting phase-modulated lasers and entangled photons as well free-space links.[45][46]

SECOQC Vienna QKD network

From 2003 to 2008 the Secure Communication based on Quantum Cryptography (SECOQC) project developed a collaborative network between a number of European institutions. The architecture chosen for the SECOQC project is a trusted repeater architecture which consists of point-to-point quantum links between devices where long distance communication is accomplished through the use of repeaters.[47]

Chinese hierarchical network

In May 2009, a hierarchical quantum network was demonstrated in Wuhu, China. The hierarchical network consists of a backbone network of four nodes connecting a number of subnets. The backbone nodes are connected through an optical switching quantum router. Nodes within each subnet are also connected through an optical switch and are connected to the backbone network through a trusted relay.[48]

Geneva area network (SwissQuantum)

The SwissQuantum network developed and tested between 2009 and 2011 linked facilities at CERN with the University of Geneva and hepia in Geneva. The SwissQuantum program focused on transitioning the technologies developed in the SECOQC and other research quantum networks into a production environment. In particular the integration with existing telecommunication networks, and its reliability and robustness.[49]

Tokyo QKD network

In 2010, a number of organizations from Japan and the European Union setup and tested the Tokyo QKD network. The Tokyo network build upon existing QKD technologies and adopted a SECOQC like network architecture. For the first time, one-time-pad encryption was implemented at high enough data rates to support popular end-user application such as secure voice and video conferencing. Previous large-scale QKD networks typically used classical encryption algorithms such as AES for high-rate data transfer and use the quantum-derived keys for low rate data or for regularly re-keying the classical encryption algorithms.[50]

Beijing-Shanghai Trunk Line

In September 2017, a 2000-km quantum key distribution network between Beijing and Shanghai, China, was officially opened. This trunk line will serve as a backbone connecting quantum networks in Beijing, Shanghai, Jinan in Shandong province and Hefei in Anhui province. During the opening ceremony, two employees from the Bank of Communications completed a transaction from Shanghai to Beijing using the network. The State Grid Corporation of China is also developing a managing application for the link.[51] The line uses 32 trusted nodes as repeaters.[52] A quantum telecommunication network has been also put into service in Wuhan, capital of central China's Hubei Province, which will be connected to the trunk. Other similar city quantum networks along the Yangtze River are planned to follow.[53]
In 2021, researchers working on this network of networks reported that they combined over 700 optical fibers with two QKD-ground-to-satellite links using a trusted relay structure for a total distance between nodes of up to ~4,600 km, which makes it Earth's largest integrated quantum communication network.[54][55]

IQNET

IQNET (Intelligent Quantum Networks and Technologies) was founded in 2017 by Caltech and AT&T. Together, they are collaborating with the Fermi National Accelerator Laboratory, and the Jet Propulsion Laboratory.[56] In December 2020, IQNET published a work in PRX Quantum that reported a successful

teleportation of time-bin qubits across 44 km of fiber.[57] For the first time, the published work includes a theoretical modelling of the experimental setup. The two test beds for performed measurements were the Caltech Quantum Network and the Fermilab Quantum Network. This research represents an important step in establishing a quantum internet of the future, which would revolutionise the fields of secure communication, data storage, precision sensing, and computing.[58]

See also

- Quantum mechanics
- Quantum computer
- Quantum bus

References

1. Kimble, H. J. (2008-06-19). "The quantum internet". *Nature*. **453** (7198): 1023–1030. arXiv:0806.4195 (https://arxiv.org/abs/0806.4195). Bibcode:2008Natur.453.1023K (https://ui.adsabs.harvard.edu/abs/2008Natur.453.1023K). doi:10.1038/nature07127 (https://doi.org/10.1038%2Fnature07127). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 18563153 (https://pubmed.ncbi.nlm.nih.gov/18563153). S2CID 4404773 (https://api.semanticscholar.org/CorpusID:4404773).
2. Caleffi, Marcello; Cacciapuoti, Angela Sara; Bianchi, Giuseppe (5 September 2018). *Quantum internet: from communication to distributed computing!*. NANOCOM '18 Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication. Reykjavik, Iceland: ACM. arXiv:1805.04360 (https://arxiv.org/abs/1805.04360). doi:10.1145/3233188.3233224 (https://doi.org/10.1145%2F3233188.3233224).
3. "The Quantum Internet Will Blow Your Mind. Here's What It Will Look Like" (https://www.discovermagazine.com/technology/the-quantum-internet-will-blow-your-mind-heres-what-it-will-look-like). *Discover Magazine*. Retrieved 2020-10-09.
4. Pednault, Edwin; Gunnels, John A.; Nannicini, Giacomo; Horesh, Lior; Magerlein, Thomas; Solomonik, Edgar; Wisnieff, Robert (2017-10-16). "Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits". arXiv:1710.05867 (https://arxiv.org/abs/1710.05867) [quant-ph (https://arxiv.org/archive/quant-ph)].
5. Van Meter, Rodney (2014). *Quantum Networking*. Hoboken: Wiley. pp. 127–196. ISBN 9781118648926. OCLC 879947342 (https://search.worldcat.org/oclc/879947342).
6. Cramer, J.; Kalb, N.; Rol, M. A.; Hensen, B.; Blok, M. S.; Markham, M.; Twitchen, D. J.; Hanson, R.; Taminiau, T. H. (2016-05-05). "Repeated quantum error correction on a continuously encoded qubit by real-time feedback" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4858808). *Nature Communications*. **7**: ncomms11526. arXiv:1508.01388 (https://arxiv.org/abs/1508.01388). Bibcode:2016NatCo...711526C (https://ui.adsabs.harvard.edu/abs/2016NatCo...711526C). doi:10.1038/ncomms11526 (https://doi.org/10.1038%2Fncomms11526). PMC 4858808 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4858808). PMID 27146630 (https://pubmed.ncbi.nlm.nih.gov/27146630).
7. Hensen, B.; Bernien, H.; Dréau, A. E.; Reiserer, A.; Kalb, N.; Blok, M. S.; Ruitenberg, J.; Vermeulen, R. F. L.; Schouten, R. N. (2015-10-29). "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". *Nature*. **526** (7575): 682–686. arXiv:1508.05949 (https://arxiv.org/abs/1508.05949). Bibcode:2015Natur.526..682H (https://ui.adsabs.harvard.edu/abs/2015Natur.526..682H). doi:10.1038/nature15759 (https://doi.org/10.1038%2Fnature15759). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 26503041 (https://pubmed.ncbi.nlm.nih.gov/26503041). S2CID 205246446 (https://api.semanticscholar.org/CorpusID:205246446).
8. Pompili, M.; Hermans, S. L. N.; Baier, S.; Beukers, H. K. C.; Humphreys, P. C.; Schouten, R. N.; Vermeulen, R. F. L.; Tiggelman, M. J.; dos Santos Martins, L.; Dirkse, B.; Wehner, S.; Hanson, R. (16 April 2021). "Realization of a multinode quantum network of remote solid-state qubits". *Science*. **372** (6539): 259–264. arXiv:2102.04471 (https://arxiv.org/abs/2102.04471). Bibcode:2021Sci...372..259P (https://ui.adsabs.harvard.edu/abs/2021Sci...372..259P). doi:10.1126/science.abg1919 (https://doi.org/10.1126%2Fscience.abg1919). PMID 33859028 (https://pubmed.ncbi.nlm.nih.gov/33859028). S2CID 231855580 (https://api.semanticscholar.org/CorpusID:231855580).
9. Pfaff, Wolfgang; Hensen, Bas; Bernien, Hannes; van Dam, Suzanne B.; Blok, Machiel S.; Taminiau, Tim H.; Tiggelman, Marijn J.; Schouten, Raymond N.; Markham, Matthew (2014-08-01). "Unconditional quantum teleportation between distant solid-state qubits". *Science*. **345** (6196): 532–535. arXiv:1404.4369 (https://arxiv.org/abs/1404.4369). Bibcode:2014Sci...345..532P (https://ui.adsabs.harvard.edu/abs/2014Sci...345..532P). doi:10.1126/science.1253512 (https://doi.org/10.1126%2Fscience.1253512). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 25082696 (https://pubmed.ncbi.nlm.nih.gov/25082696). S2CID 2190249 (https://api.semanticscholar.org/CorpusID:2190249).

10. Inlek, I. V.; Crocker, C.; Lichtman, M.; Sosnova, K.; Monroe, C. (2017-06-23). "Multispecies Trapped-Ion Node for Quantum Networking". *Physical Review Letters*. **118** (25): 250502. arXiv:1702.01062 (https://arxiv.org/abs/1702.01062). Bibcode:2017PhRvL.118y0502I (https://ui.adsabs.harvard.edu/abs/2017PhRvL.118y0502I). doi:10.1103/PhysRevLett.118.250502 (https://doi.org/10.1103%2FPhysRevLett.118.250502). PMID 28696766 (https://pubmed.ncbi.nlm.nih.gov/28696766). S2CID 44046802 (https://api.semanticscholar.org/CorpusID:44046802).
11. Pellizzari, T; Gardiner, SA; Cirac, JI; Zoller, P (1995), "Decoherence, continuous observation, and quantum computing: A cavity QED model", *Physical Review Letters*, **75** (21): 3788–3791, Bibcode:1995PhRvL..75.3788P (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75.3788P), doi:10.1103/physrevlett.75.3788 (https://doi.org/10.1103%2Fphysrevlett.75.3788), PMID 10059732 (https://pubmed.ncbi.nlm.nih.gov/10059732)
12. Ritter, Stephan; Nölleke, Christian; Hahn, Carolin; Reiserer, Andreas; Neuzner, Andreas; Uphoff, Manuel; Müicke, Martin; Figueroa, Eden; Bochmann, Joerg; Rempe, Gerhard (2012), "An elementary quantum network of single atoms in optical cavities", *Nature*, **484** (7393): 195–200, arXiv:1202.5955 (https://arxiv.org/abs/1202.5955), Bibcode:2012Natur.484..195R (https://ui.adsabs.harvard.edu/abs/2012Natur.484..195R), doi:10.1038/nature11023 (https://doi.org/10.1038%2Fnature11023), PMID 22498625 (https://pubmed.ncbi.nlm.nih.gov/22498625), S2CID 205228562 (https://api.semanticscholar.org/CorpusID:205228562)
13. Gisson, Nicolas; Ribordy, Grégoire; Tittel, Wolfgang; Zbinden, Hugo (2002), "Quantum cryptography", *Reviews of Modern Physics*, **74** (1): 145, arXiv:quant-ph/0101098 (https://arxiv.org/abs/quant-ph/0101098), Bibcode:2002RvMP...74..145G (https://ui.adsabs.harvard.edu/abs/2002RvMP...74..145G), doi:10.1103/revmodphys.74.145 (https://doi.org/10.1103%2Frevmodphys.74.145), S2CID 6979295 (https://api.semanticscholar.org/CorpusID:6979295)
14. Yirka, Bob (February 13, 2020). "Quantum memories entangled over 50-kilometer cable" (https://phys.org/news/2020-02-quantum-memories-entangled-kilometer-cable.html). *Nature*. **578** (7794): 240–245. arXiv:1903.11284 (https://arxiv.org/abs/1903.11284). doi:10.1038/s41586-020-1976-7 (https://doi.org/10.1038%2Fs41586-020-1976-7). PMID 32051600 (https://pubmed.ncbi.nlm.nih.gov/32051600). S2CID 211089074 (https://api.semanticscholar.org/CorpusID:211089074).
15. Hughes, Richard J; Nordholt, Jane E; Derkacs, Derek; Peterson, Charles G (2002), "Practical free-space quantum key distribution over 10 km in daylight and at night", *New Journal of Physics*, **4** (1): 43, arXiv:quant-ph/0206092 (https://arxiv.org/abs/quant-ph/0206092), Bibcode:2002NJPh....4...43H (https://ui.adsabs.harvard.edu/abs/2002NJPh....4...43H), doi:10.1088/1367-2630/4/1/343 (https://doi.org/10.1088%2F1367-2630%2F4%2F1%2F343), S2CID 119468993 (https://api.semanticscholar.org/CorpusID:119468993)
16. Yin, Juan; Cao, Yuan; Li, Yu-Huai; Liao, Sheng-Kai; Zhang, Liang; Ren, Ji-Gang; Cai, Wen-Qi; Liu, Wei-Yue; Li, Bo (2017-07-05). "Satellite-Based Entanglement Distribution Over 1200 kilometers". *Science*. **356** (2017): 1140–1144. arXiv:1707.01339 (https://arxiv.org/abs/1707.01339). Bibcode:2017arXiv170701339Y (https://ui.adsabs.harvard.edu/abs/2017arXiv170701339Y). doi:10.1126/science.aan3211 (https://doi.org/10.1126%2Fscience.aan3211). PMID 28619937 (https://pubmed.ncbi.nlm.nih.gov/28619937). S2CID 5206894 (https://api.semanticscholar.org/CorpusID:5206894).
17. Calderaro, Luca; Agnesi, Costantino; Dequal, Daniele; Vedovato, Francesco; Schiavon, Matteo; Santamato, Alberto; Luceri, Vincenza; Bianco, Giuseppe; Vallone, Giuseppe; Villoresi, Paolo (2019). "Towards quantum communication from global navigation satellite system". *Quantum Science and Technology*. **4** (1): 015012. arXiv:1804.05022 (https://arxiv.org/abs/1804.05022). Bibcode:2019QS&T....4a5012C (https://ui.adsabs.harvard.edu/abs/2019QS&T....4a5012C). doi:10.1088/2058-9565/aaefd4 (https://doi.org/10.1088%2F2058-9565%2Faaefd4). S2CID 55395441 (https://api.semanticscholar.org/CorpusID:55395441).
18. Bouwmeester, Dik; Pan, Jian-Wei; Mattle, Klaus; Eibl, Manfred; Weinfurter, Harald; Zeilinger, Anton (1997), "Experimental quantum teleportation", *Nature*, **390** (6660): 575–579, arXiv:1901.11004 (https://arxiv.org/abs/1901.11004), Bibcode:1997Natur.390..575B (https://ui.adsabs.harvard.edu/abs/1997Natur.390..575B), doi:10.1038/37539 (https://doi.org/10.1038%2F37539), S2CID 4422887 (https://api.semanticscholar.org/CorpusID:4422887)
19. Sangouard, Nicolas; Simon, Christoph; De Riedmatten, Hugues; Gisin, Nicolas (2011), "Quantum repeaters based on atomic ensembles and linear optics", *Reviews of Modern Physics*, **83** (1): 33–80, arXiv:0906.2699 (https://arxiv.org/abs/0906.2699), Bibcode:2011RvMP...83...33S (https://ui.adsabs.harvard.edu/abs/2011RvMP...83...33S), doi:10.1103/revmodphys.83.33 (https://doi.org/10.1103%2Frevmodphys.83.33), S2CID 118407183 (https://api.semanticscholar.org/CorpusID:118407183)
20. Krutyanskiy, V.; Canteri, M.; Meraner, M.; Bate, J.; Krcmarsky, V.; Schupp, J.; Sangouard, N.; Lanyon, B. P. (2023-05-22). "Telecom-Wavelength Quantum Repeater Node Based on a Trapped-Ion Processor" (https://link.aps.org/doi/10.1103/PhysRevLett.130.213601). *Physical Review Letters*. **130** (21): 213601. arXiv:2210.05418 (https://arxiv.org/abs/2210.05418). Bibcode:2023PhRvL.130u3601K (https://ui.adsabs.harvard.edu/abs/2023PhRvL.130u3601K). doi:10.1103/PhysRevLett.130.213601 (https://doi.org/10.1103%2FPhysRevLett.130.213601). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 37295084 (https://pubmed.ncbi.nlm.nih.gov/37295084). S2CID 252816066 (https://api.semanticscholar.org/CorpusID:252816066).

21. Nunn, Joshua (2017-05-24). "Viewpoint: A Solid Footing for a Quantum Repeater" (https://physics.aps.org/featured-article-pdf/10.1103/PhysRevLett.118.210501). *Physics*. **10**: 55. Bibcode:2017PhyOJ..10...55N (https://ui.adsabs.harvard.edu/abs/2017PhyOJ..10...55N). doi:10.1103/physics.10.55 (https://doi.org/10.1103%2Fphysics.10.55).
22. Muralidharan, Sreraman; Li, Linshu; Kim, Jungsang; Lutkenhaus, Norbert; Lukin, Mikhail; Jiang, Liang (2016), "Optimal architectures for long distance quantum communication", *Scientific Reports*, **6**, Nature: 20463, Bibcode:2016NatSR...620463M (https://ui.adsabs.harvard.edu/abs/2016NatSR...620463M), doi:10.1038/srep20463 (https://doi.org/10.1038%2Fsrep20463), PMC 4753438 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4753438), PMID 26876670 (https://pubmed.ncbi.nlm.nih.gov/26876670)
23. Kalb, Norbert; Reiserer, Andreas A.; Humphreys, Peter C.; Bakermans, Jacob J. W.; Kamerling, Sten J.; Nickerson, Naomi H.; Benjamin, Simon C.; Twitchen, Daniel J.; Markham, Matthew (2017-06-02). "Entanglement Distillation between Solid-State Quantum Network Nodes". *Science*. **356** (6341): 928–932. arXiv:1703.03244 (https://arxiv.org/abs/1703.03244). Bibcode:2017Sci...356..928K (https://ui.adsabs.harvard.edu/abs/2017Sci...356..928K). doi:10.1126/science.aan0070 (https://doi.org/10.1126%2Fscience.aan0070). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 28572386 (https://pubmed.ncbi.nlm.nih.gov/28572386). S2CID 206658460 (https://api.semanticscholar.org/CorpusID:206658460).
24. Sasaki, Masahide (2017). "Quantum networks: where should we be heading?" (https://doi.org/10.1088%2F2058-9565%2Faa6994). *Quantum Science and Technology*. **2** (2): 020501. Bibcode:2017QS&T....2b0501S (https://ui.adsabs.harvard.edu/abs/2017QS&T....2b0501S). doi:10.1088/2058-9565/aa6994 (https://doi.org/10.1088%2F2058-9565%2Faa6994). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565).
25. Tajima, A; Kondoh, T; Fujiwara, M; Yoshino, K; Iizuka, H; Sakamoto, T; Tomita, A; Shimamura, E; Asami, S; Sasaki, M (2017). "Quantum key distribution network for multiple applications". *Quantum Science and Technology*. **2** (3): 034003. Bibcode:2017QS&T....2c4003T (https://ui.adsabs.harvard.edu/abs/2017QS&T....2c4003T). doi:10.1088/2058-9565/aa7154 (https://doi.org/10.1088%2F2058-9565%2Faa7154). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 57545550 (https://api.semanticscholar.org/CorpusID:57545550).
26. Kómár, P.; Kessler, E. M.; Bishof, M.; Jiang, L.; Sørensen, A. S.; Ye, J.; Lukin, M. D. (2014-06-15). "A quantum network of clocks". *Nature Physics*. **10** (8): 582–587. arXiv:1310.6045 (https://arxiv.org/abs/1310.6045). Bibcode:2014NatPh..10..582K (https://ui.adsabs.harvard.edu/abs/2014NatPh..10..582K). doi:10.1038/nphys3000 (https://doi.org/10.1038%2Fnphys3000). ISSN 1745-2481 (https://search.worldcat.org/issn/1745-2481). S2CID 16355907 (https://api.semanticscholar.org/CorpusID:16355907).
27. Gottesman, Daniel; Jennewein, Thomas; Croke, Sarah (2012-08-16). "Longer-Baseline Telescopes Using Quantum Repeaters". *Physical Review Letters*. **109** (7): 070503. arXiv:1107.2939 (https://arxiv.org/abs/1107.2939). Bibcode:2012PhRvL.109g0503G (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109g0503G). doi:10.1103/PhysRevLett.109.070503 (https://doi.org/10.1103%2FPhysRevLett.109.070503). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 23006349 (https://pubmed.ncbi.nlm.nih.gov/23006349). S2CID 20073853 (https://api.semanticscholar.org/CorpusID:20073853).
28. Khabiboulline, E. T.; Borregaard, J.; De Greve, K.; Lukin, M. D. (2019). "Quantum-assisted telescope arrays". *Physical Review A*. **100** (2): 022316. arXiv:1809.03396 (https://arxiv.org/abs/1809.03396). Bibcode:2019PhRvA.100b2316K (https://ui.adsabs.harvard.edu/abs/2019PhRvA.100b2316K). doi:10.1103/PhysRevA.100.022316 (https://doi.org/10.1103%2FPhysRevA.100.022316).
29. Malaney, Robert (2016). "The Quantum Car" (https://ieeexplore.ieee.org/document/7563890). *IEEE Wireless Communications Letters*. **5** (6): 624–627. arXiv:1512.03521 (https://arxiv.org/abs/1512.03521). doi:10.1109/LWC.2016.2607740 (https://doi.org/10.1109%2FLWC.2016.2607740). S2CID 2483729 (https://api.semanticscholar.org/CorpusID:2483729).
30. Buhrman, Harry; Nishanth, Chandran; Fehr, Serge; Ran, Gelles; Vipul, Goyal; Ostrovsky, Rafail; Schaffner, Christian (2014). "Position-based quantum cryptography: Impossibility and constructions" (https://dare.uva.nl/personal/pure/en/publications/positionbased-quantum-cryptography-impossibility-and-constructions(967acc8e-a0e0-43b2-b603-3c66bd69cf65).html). *SIAM*. **43**: 150–178. arXiv:1009.2490 (https://arxiv.org/abs/1009.2490). doi:10.1137/130913687 (https://doi.org/10.1137%2F130913687).
31. Broadbent, Anne; Fitzsimons, Joseph; Kashefi, Elham (2009–2010). "Universal Blind Quantum Computation" (https://ieeexplore.ieee.org/document/5438603). *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. pp. 517–526. arXiv:0807.4154 (https://arxiv.org/abs/0807.4154). doi:10.1109/FOCS.2009.36 (https://doi.org/10.1109%2FFOCS.2009.36). hdl:20.500.11820/11ca3f3d-e712-466a-a16d-74088b2675fa (https://hdl.handle.net/20.500.11820%2F11ca3f3d-e712-466a-a16d-74088b2675fa). ISBN 978-1-4244-5116-6. S2CID 650251 (https://api.semanticscholar.org/CorpusID:650251).
32. Mastorakis, Nikos E. *Networks and Quantum Computing*. Nova Science Publishers, 2012.
33. Ananthaswamy, Anil (August 2019). "The Quantum Internet Is Emerging, One Experiment at a Time" (https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/). *Scientific American*. Retrieved 2020-10-12.

34. Leprince-Ringuet, Daphne. "What is the quantum internet? Everything you need to know about the weird future of quantum networks" (https://www.zdnet.com/article/what-is-the-quantum-internet-everything-you-need-to-know-about-the-weird-future-of-quantum-networks/). *ZDNet*. Retrieved 2020-10-12.
35. "Multi-user communication network paves the way towards the quantum internet" (https://physicsworld.com/a/multi-user-communication-network-paves-the-way-towards-the-quantum-internet/). *Physics World*. 8 September 2020. Retrieved 8 October 2020.
36. Joshi, Siddarth Koduru; Aktas, Djeylan; Wengerowsky, Sören; Lončarić, Martin; Neumann, Sebastian Philipp; Liu, Bo; Scheidl, Thomas; Lorenzo, Guillermo Currás; Samec, Željko; Kling, Laurent; Qiu, Alex; Razavi, Mohsen; Stipčević, Mario; Rarity, John G.; Ursin, Rupert (1 September 2020). "A trusted node–free eight-user metropolitan quantum communication network" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7467697). *Science Advances*. **6** (36): eaba0959. arXiv:1907.08229 (https://arxiv.org/abs/1907.08229). Bibcode:2020SciA....6..959J (https://ui.adsabs.harvard.edu/abs/2020SciA....6..959J). doi:10.1126/sciadv.aba0959 (https://doi.org/10.1126%2Fsciadv.aba0959). ISSN 2375-2548 (https://search.worldcat.org/issn/2375-2548). PMC 7467697 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7467697). PMID 32917585 (https://pubmed.ncbi.nlm.nih.gov/32917585). Text and images are available under a Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/).
37. Fardelli, Ingrid (August 17, 2022). "The entanglement of two quantum memory systems 12.5 km apart from each other" (https://phys.org/news/2022-08-entanglement-quantum-memory-km.amp). Phys.org.
38. Metz, Cade (2022-05-25). " 'Quantum Internet' Inches Closer With Advance in Data Teleportation" (https://www.nytimes.com/2022/05/25/technology/quantum-internet-teleportation.html). *The New York Times*. ISSN 0362-4331 (https://search.worldcat.org/issn/0362-4331). Retrieved 2022-05-26.
39. Dunning, Hayley (April 17, 2024). "Crucial connection for 'quantum internet' made for the first time" (https://www.imperial.ac.uk/news/252621/crucial-connection-quantum-internet-made-first/).
40. "Quantum systems learn joint computing" (https://phys.org/news/2021-02-quantum-joint.html). *phys.org*. Retrieved 7 March 2021.
41. Daiss, Severin; Langenfeld, Stefan; Welte, Stephan; Distante, Emanuele; Thomas, Philip; Hartung, Lukas; Morin, Olivier; Rempe, Gerhard (5 February 2021). "A quantum-logic gate between distant quantum-network modules" (https://www.science.org/doi/10.1126/science.abe3150). *Science*. **371** (6529): 614–617. arXiv:2103.13095 (https://arxiv.org/abs/2103.13095). Bibcode:2021Sci...371..614D (https://ui.adsabs.harvard.edu/abs/2021Sci...371..614D). doi:10.1126/science.abe3150 (https://doi.org/10.1126%2Fscience.abe3150). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33542133 (https://pubmed.ncbi.nlm.nih.gov/33542133). S2CID 231808141 (https://api.semanticscholar.org/CorpusID:231808141). Retrieved 7 March 2021.
42. Jarrah, Katharina (November 5, 2020). "Physicists develop efficient modem for a future quantum internet" (https://phys.org/news/2020-11-physicists-efficient-modem-future-quantum.html). *Phys.org*. Retrieved November 5, 2020.
43. "Using drones to create local quantum networks" (https://phys.org/news/2021-01-drones-local-quantum-networks.html). *phys.org*. Retrieved 12 February 2021.
44. Liu, Hua-Ying; Tian, Xiao-Hui; Gu, Changsheng; Fan, Pengfei; Ni, Xin; Yang, Ran; Zhang, Ji-Ning; Hu, Mingzhe; Guo, Jian; Cao, Xun; Hu, Xiaopeng; Zhao, Gang; Lu, Yan-Qing; Gong, Yan-Xiao; Xie, Zhenda; Zhu, Shi-Ning (15 January 2021). "Optical-Relayed Entanglement Distribution Using Drones as Mobile Nodes" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.126.020503). *Physical Review Letters*. **126** (2): 020503. Bibcode:2021PhRvL.126b0503L (https://ui.adsabs.harvard.edu/abs/2021PhRvL.126b0503L). doi:10.1103/PhysRevLett.126.020503 (https://doi.org/10.1103%2FPhysRevLett.126.020503). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 33512193 (https://pubmed.ncbi.nlm.nih.gov/33512193). S2CID 231761406 (https://api.semanticscholar.org/CorpusID:231761406). Retrieved 12 February 2021.
45. Elliot, Chip (2002), "Building the quantum network", *New Journal of Physics*, **4** (1): 46, Bibcode:2002NJPh....4...46E (https://ui.adsabs.harvard.edu/abs/2002NJPh....4...46E), doi:10.1088/1367-2630/4/1/346 (https://doi.org/10.1088%2F1367-2630%2F4%2F1%2F346)
46. Elliott, Chip; Colvin, Alexander; Pearson, David; Pikalo, Oleksiy; Schlafer, John; Yeh, Henry (2005), "Current status of the DARPA Quantum Network", *Defense and Security*, International Society for Optics and Photonics: 138–149
47. Peev, Momtchil; Pacher, Christoph; Alléaume, Romain; Barreiro, Claudio; Bouda, Jan; Boxleitner, W; Debuisschert, Thierry; Diamanti, Eleni; Dianati, M; Dynes, JF (2009), "The SECOQC quantum key distribution network in Vienna", *New Journal of Physics*, **11** (7), IOP Publishing: 075001, Bibcode:2009NJPh...11g5001P (https://ui.adsabs.harvard.edu/abs/2009NJPh...11g5001P), doi:10.1088/1367-2630/11/7/075001 (https://doi.org/10.1088%2F1367-2630%2F11%2F7%2F075001)

48. Xu, FangXing; Chen, Wei; Wang, Shuang; Yin, ZhenQiang; Zhang, Yang; Liu, Yun; Zhou, Zheng; Zhao, YiBo; Li, HongWei; Liu, Dong (2009), "Field experiment on a robust hierarchical metropolitan quantum cryptography network", *Chinese Science Bulletin*, **54** (17), Springer: 2991–2997, arXiv:0906.3576 (https://arxiv.org/abs/0906.3576), Bibcode:2009ChSBu..54.2991X (https://ui.adsabs.harvard.edu/abs/2009ChSBu..54.2991X), doi:10.1007/s11434-009-0526-3 (https://doi.org/10.1007%2Fs11434-009-0526-3), S2CID 118300112 (https://api.semanticscholar.org/CorpusID:118300112)
49. Stucki, Damien; Legre, Matthieu; Buntschu, F; Clausen, B; Felber, Nadine; Gisin, Nicolas; Henzen, L; Junod, Pascal; Litzistorf, G; Monbaron, Patrick (2011). "Long-term performance of the SwissQuantum quantum key distribution network in a field environment". *New Journal of Physics*. **13** (12). IOP Publishing: 123001. arXiv:1203.4940 (https://arxiv.org/abs/1203.4940). Bibcode:2011NJPh...13l3001S (https://ui.adsabs.harvard.edu/abs/2011NJPh...13l3001S). doi:10.1088/1367-2630/13/12/123001 (https://doi.org/10.1088%2F1367-2630%2F13%2F12%2F123001). S2CID 54502793 (https://api.semanticscholar.org/CorpusID:54502793).
50. Sasaki, M; Fujiwara, M; Ishizuka, H; Klaus, W; Wakui, K; Takeoka, M; Miki, S; Yamashita, T; Wang, Z; Tanaka, A (2011), "Field test of quantum key distribution in the Tokyo QKD Network", *Optics Express*, **19** (11), Optical Society of America: 10387–10409, arXiv:1103.3566 (https://arxiv.org/abs/1103.3566), Bibcode:2011OExpr..1910387S (https://ui.adsabs.harvard.edu/abs/2011OExpr..1910387S), doi:10.1364/oe.19.010387 (https://doi.org/10.1364%2Foe.19.010387), PMID 21643295 (https://pubmed.ncbi.nlm.nih.gov/21643295), S2CID 593516 (https://api.semanticscholar.org/CorpusID:593516)
51. Zhang, Zhihao (2017-09-30). "Beijing-Shanghai quantum link a "new era" " (http://www.chinadaily.com.cn/china/2017-09/30/content_32669593.htm). China Daily.
52. Courtland, Rachel (26 Oct 2016). "China's 2,000-km Quantum Link Is Almost Complete" (https://spectrum.ieee.org/chinas-2000km-quantum-link-is-almost-complete). IEEE Spectrum: Technology, Engineering, and Science News.
53. "Quantum communication networks put in service in central China" (https://web.archive.org/web/20180328102536/http://www.xinhuanet.com/english/2017-10/31/c_136717809.htm). Xinhua. 2017-10-31. Archived from the original (http://www.xinhuanet.com/english/2017-10/31/c_136717809.htm) on March 28, 2018.
54. "The world's first integrated quantum communication network" (https://phys.org/news/2021-01-world-quantum-network.html). *phys.org*. Retrieved 11 February 2021.
55. Chen, Yu-Ao; Zhang, Qiang; Chen, Teng-Yun; Cai, Wen-Qi; Liao, Sheng-Kai; Zhang, Jun; Chen, Kai; Yin, Juan; Ren, Ji-Gang; Chen, Zhu; Han, Sheng-Long; Yu, Qing; Liang, Ken; Zhou, Fei; Yuan, Xiao; Zhao, Mei-Sheng; Wang, Tian-Yin; Jiang, Xiao; Zhang, Liang; Liu, Wei-Yue; Li, Yang; Shen, Qi; Cao, Yuan; Lu, Chao-Yang; Shu, Rong; Wang, Jian-Yu; Li, Li; Liu, Nai-Le; Xu, Feihu; Wang, Xiang-Bin; Peng, Cheng-Zhi; Pan, Jian-Wei (January 2021). "An integrated space-to-ground quantum communication network over 4,600 kilometres" (https://www.nature.com/articles/s41586-020-03093-8). *Nature*. **589** (7841): 214–219. Bibcode:2021Natur.589..214C (https://ui.adsabs.harvard.edu/abs/2021Natur.589..214C). doi:10.1038/s41586-020-03093-8 (https://doi.org/10.1038%2Fs41586-020-03093-8). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 33408416 (https://pubmed.ncbi.nlm.nih.gov/33408416). S2CID 230812317 (https://api.semanticscholar.org/CorpusID:230812317). Retrieved 11 February 2021.
56. "INQNET - press release" (https://inqnet.caltech.edu/Press-PRXQ-dec142020.html). *inqnet.caltech.edu*. Retrieved 2020-12-26.
57. Valivarthi, Raju; Davis, Samantha I.; Peña, Cristián; Xie, Si; Lauk, Nikolai; Narváez, Lautaro; Allmaras, Jason P.; Beyer, Andrew D.; Gim, Yewon; Hussein, Meraj; Iskander, George (2020-12-04). "Teleportation Systems Toward a Quantum Internet" (https://doi.org/10.1103%2FPRXQuantum.1.020317). *PRX Quantum*. **1** (2): 020317. arXiv:2007.11157 (https://arxiv.org/abs/2007.11157). Bibcode:2020PRXQ....1b0317V (https://ui.adsabs.harvard.edu/abs/2020PRXQ....1b0317V). doi:10.1103/PRXQuantum.1.020317 (https://doi.org/10.1103%2FPRXQuantum.1.020317).
58. "Quantum Internet Tested at Caltech and Fermilab" (https://www.caltech.edu/about/news/quantum-internet-tested-caltech-and-fermilab). *California Institute of Technology*. 14 December 2020. Retrieved 2020-12-26.

Further reading

- Wehner, Stephanie; Elkouss, David; Hanson, Ronald (2018). "Quantum internet: A vision for the road ahead". *Science*. **362** (6412): eaam9288. Bibcode:2018Sci...362.9288W (https://ui.adsabs.harvard.edu/abs/2018Sci...362.9288W). doi:10.1126/science.aam9288 (https://doi.org/10.1126%2Fscience.aam9288). PMID 30337383 (https://pubmed.ncbi.nlm.nih.gov/30337383). S2CID 53018298 (https://api.semanticscholar.org/CorpusID:53018298).
- Razavi, Mohsen (2018). *An Introduction to Quantum Communication Networks: Or, How Shall We Communicate in the Quantum Era?*. Morgan & Claypool Publishers. Bibcode:2018iqcn.book.....R (https://ui.adsabs.harvard.edu/abs/2018iqcn.book.....R). doi:10.1088/978-1-6817-4653-1 (https://doi.org/10.1088%2F978-1-6817-4653-1). ISBN 978-1-6817-4653-1.

- Rohde, Peter P. (2021). *The quantum internet: The second quantum revolution*. Cambridge University Press. doi:10.1017/9781108868815 (https://doi.org/10.1017%2F9781108868815). ISBN 9781108868815. S2CID 239184623 (https://api.semanticscholar.org/CorpusID:239184623).
- Wei, Shi-Hai; et al. (2022). "Towards real-world quantum networks: a review". *Laser & Photonics Reviews*. **16** (3): 2100219. arXiv:2201.04802 (https://arxiv.org/abs/2201.04802). Bibcode:2022LPRv...1600219W (https://ui.adsabs.harvard.edu/abs/2022LPRv...1600219W). doi:10.1002/lpor.202100219 (https://doi.org/10.1002%2Flpor.202100219). S2CID 245906136 (https://api.semanticscholar.org/CorpusID:245906136).
- Nokkala, Johannes; Piilo, Jyrki; Bianconi, Ginestra (2024). "Complex quantum networks: A topical review". *Journal of Physics A: Mathematical and Theoretical*. **57** (23). arXiv:2311.16265 (https://arxiv.org/abs/2311.16265). Bibcode:2024JPhA...57w3001N (https://ui.adsabs.harvard.edu/abs/2024JPhA...57w3001N). doi:10.1088/1751-8121/ad41a6 (https://doi.org/10.1088%2F1751-8121%2Fad41a6).

External links

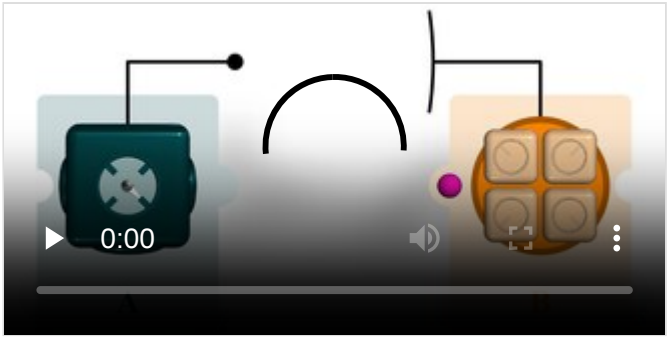
- https://web.archive.org/web/20090716121402/http://itvibe.com/news/2583/
- http://www.vnunet.com/vnunet/news/2125164/first-quantum-computr-network-goes-online
- Elliott, Chip (2004). "The DARPA Quantum Network". arXiv:quant-ph/0412029 (https://arxiv.org/abs/quant-ph/0412029).
- http://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/
- https://web.archive.org/web/20141229113448/http://www.ipod.org.uk/reality/reality_quantum_entanglement.asp

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_network&oldid=1239680109"

WIKIPEDIA
The Free Encyclopedia

Quantum teleportation

Quantum teleportation is a technique for transferring quantum information from a sender at one location to a receiver some distance away. While teleportation is commonly portrayed in science fiction as a means to transfer physical objects from one location to the next, quantum teleportation only transfers quantum information. The sender does not have to know the particular quantum state being transferred. Moreover, the location of the recipient can be unknown, but to complete the quantum teleportation, classical information needs to be sent from sender to receiver. Because classical information needs to be sent, quantum teleportation cannot occur faster than the speed of light.



Schematic video demonstrating individual steps of quantum teleportation. A quantum state Q is sent from station A to station B using a pair of entangled particles created by source S. Station A measures its two particles and communicates the result to station B, which chooses an appropriate device based on the received message. Due to the action of the device, the state of the particle of station B turns into Q.

One of the first scientific articles to investigate quantum teleportation is "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels"[1] published by C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters in 1993, in which they proposed using dual communication methods to send/receive quantum information. It was experimentally realized in 1997 by two research groups, led by Sandu Popescu and Anton Zeilinger, respectively.[2][3]

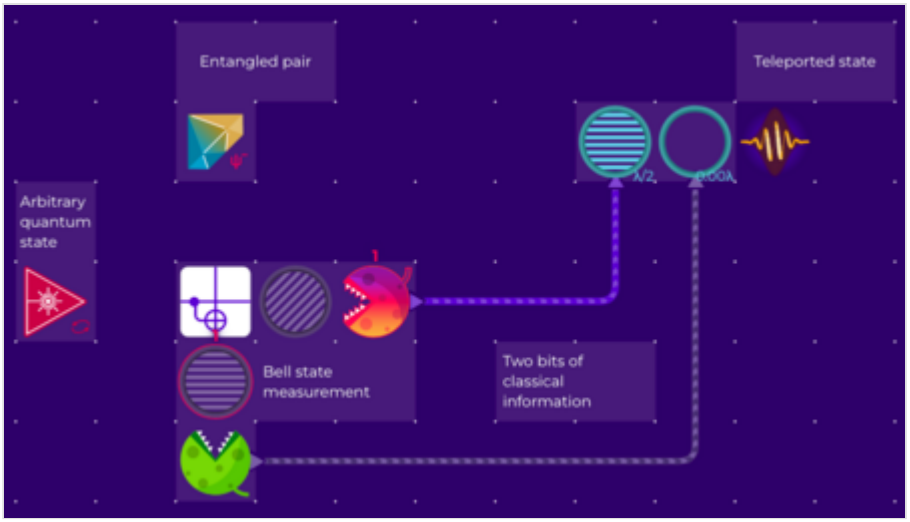
Experimental determinations[4][5] of quantum teleportation have been made in information content – including photons, atoms, electrons, and superconducting circuits – as well as distance, with 1,400 km (870 mi) being the longest distance of successful teleportation by Jian-Wei Pan's team using the Micius satellite for space-based quantum teleportation.[6]

Non-technical summary

In matters relating to quantum information theory, it is convenient to work with the simplest possible unit of information: the two-state system of the qubit. The qubit functions as the quantum analog of the classic computational part, the bit, as it can have a measurement value of *both* a 0 *and* a 1, whereas the classical bit can only be measured as a 0 *or* a 1. The quantum two-state system seeks to transfer quantum information from one location to another location without losing the information and preserving the quality of this information. This process involves moving the information *between carriers* and not movement of the *actual carriers*, similar to the traditional process of communications, as two parties remain stationary while the information (digital media, voice, text, etc.) is being transferred, contrary to the implications of the word "teleport". The main components needed for teleportation include a sender, the information (a qubit), a traditional channel, a quantum channel, and a receiver. The sender does not

need to know the exact contents of the information being sent. The measurement postulate of quantum mechanics – when a measurement is made upon a quantum state, any subsequent measurements will "collapse" or that the observed state will be lost – creates an imposition within teleportation: if a sender measures their information, the state could collapse when the receiver obtains the data since the state had changed from when the sender made the initial measurement and in so making it different.

For actual teleportation, it is required that an entangled quantum state be created for the qubit to be transferred. Entanglement imposes statistical correlations between otherwise distinct physical systems by creating or placing two or more separate particles into a single, shared quantum state. This intermediate state contains two particles whose quantum states are related to each other: measuring one particle's state provides information about the measurement of the other particle's state. These correlations hold even when measurements are chosen and performed independently, out of causal contact from one another, as verified in Bell test experiments. Thus, an observation resulting from a measurement choice made at one point in spacetime seems to instantaneously affect outcomes in another region, even though light hasn't yet had time to travel the distance, a conclusion seemingly at odds with special relativity. This is known as the EPR paradox. However, such correlations can never be used to transmit any information faster than the speed of light, a statement encapsulated in the no-communication theorem. Thus, teleportation as a whole can never be superluminal, as a qubit cannot be reconstructed until the accompanying classical information arrives.



An interactive simulation of quantum teleportation in the Virtual Lab by Quantum Flytrap,[7] available online (https://lab.quantumflytrap.com/lab/quantum-teleportation). In this optical setup, qubits are encoded using the polarization of light. Teleportation occurs between the source photon (set to an arbitrary state) and one photon from an entangled pair. A Bell pair measurement is performed on the source photon and one entangled photon using a quantum CNOT gate, yielding two bits of classical information. The target photon is then rotated with two controllable waveplates based on this information.

The sender will combine the particle, of which the information is teleported, with one of the entangled particles, causing a change of the overall entangled quantum state. Of this changed state, the particles in receiver's possession are then sent to an analyzer that will measure the change of the entangled state. The "change" measurement will allow the receiver to recreate the original information that the sender had, resulting in the information being teleported or carried between two people that have different locations. Since the initial quantum information is "destroyed" as it becomes part of the entanglement state, the no-cloning theorem is maintained as the information is recreated from the entangled state and not copied during teleportation.

The quantum channel is the communication mechanism that is used for all quantum information transmission and is the channel used for teleportation (relationship of quantum channel to traditional communication channel is akin to the qubit being the quantum analog of the classical bit). However, in addition to the quantum channel, a traditional channel must also be used to accompany a qubit to "preserve" the quantum information. When the change measurement between the original qubit and the entangled particle is made, the measurement result must be carried by a traditional channel so that the quantum information can be reconstructed and the receiver can get the original information. Because of this need for the traditional channel, the speed of teleportation can be no faster than the speed of light (hence the no-communication theorem is not violated). The main advantage with this is that Bell states can be shared using photons from lasers, making teleportation achievable through open space, as there is no need to send information through physical cables or optical fibers.

Quantum states can be encoded in various degrees of freedom of atoms. For example, qubits can be encoded in the degrees of freedom of electrons surrounding the atomic nucleus or in the degrees of freedom of the nucleus itself. Thus, performing this kind of teleportation requires a stock of atoms at the receiving site, available for having qubits imprinted on them.[8]

As of 2015, the quantum states of single photons, photon modes, single atoms, atomic ensembles, defect centers in solids, single electrons, and superconducting circuits have been employed as information bearers.[9]

Understanding quantum teleportation requires a good grounding in finite-dimensional linear algebra, Hilbert spaces and projection matrixes. A qubit is described using a two-dimensional complex number-valued vector space (a Hilbert space), which are the primary basis for the formal manipulations given below. A working knowledge of quantum mechanics is not absolutely required to understand the mathematics of quantum teleportation, although without such acquaintance, the deeper meaning of the equations may remain quite mysterious.

Protocol

The resources required for quantum teleportation are a communication channel capable of transmitting two classical bits, a means of generating an entangled Bell state of qubits and distributing to two different locations, performing a Bell measurement on one of the Bell state qubits, and manipulating the quantum state of the other qubit from the pair. Of course, there must also be some input qubit (in the quantum state $|\phi\rangle$) to be teleported. The protocol is then as follows:

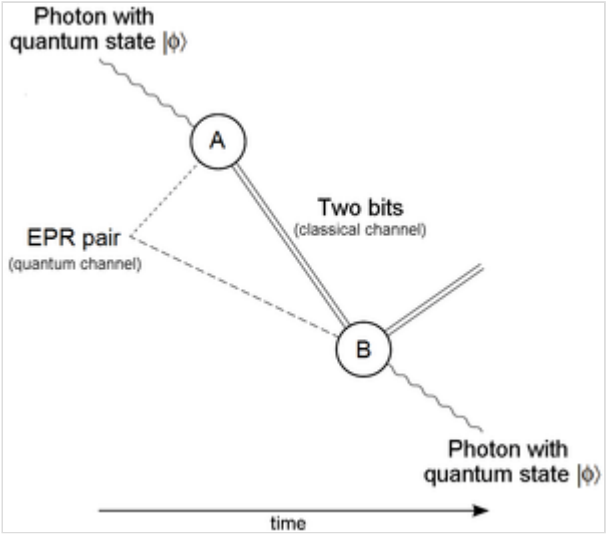


Diagram for quantum teleportation of a photon

1. A Bell state is generated with one qubit sent to location A and the other sent to location B.
2. A Bell measurement of the Bell state qubit and the qubit to be teleported ($|\phi\rangle$) is performed at location A. This yields one of four measurement outcomes which can be encoded in two classical bits of information. Both qubits at location A are then discarded.

3. Using the classical channel, the two bits are sent from A to B. (This is the only potentially time-consuming step after step 1 since information transfer is limited by the speed of light.)
4. As a result of the measurement performed at location A, the Bell state qubit at location B is in one of four possible states. Of these four possible states, one is identical to the original quantum state $|\phi\rangle$, and the other three are closely related. The identity of the state actually obtained is encoded in two classical bits and sent to location B. The Bell state qubit at location B is then modified in one of three ways, or not at all, which results in a qubit identical to $|\phi\rangle$, the state of the qubit that was chosen for teleportation.

It is worth noticing that the above protocol assumes that the qubits are individually addressable, meaning that the qubits are distinguishable and physically labeled. However, there can be situations where two identical qubits are indistinguishable due to the spatial overlap of their wave functions. Under this condition, the qubits cannot be individually controlled or measured. Nevertheless, a teleportation protocol analogous to that described above can still be (conditionally) implemented by exploiting two independently prepared qubits, with no need of an initial Bell state. This can be made by addressing the internal degrees of freedom of the qubits (e.g., spins or polarisations) by spatially localized measurements performed in separated regions A and B where the two spatially overlapping, indistinguishable qubits can be found.[10] This theoretical prediction has been then verified experimentally via polarized photons in a quantum optical setup.[11]

Experimental results and records

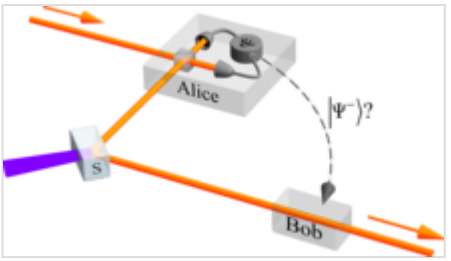
Work in 1998 verified the initial predictions,[2] and the distance of teleportation was increased in August 2004 to 600 meters, using optical fiber.[12] Subsequently, the record distance for quantum teleportation has been gradually increased to 16 kilometres (9.9 mi),[13] then to 97 km (60 mi),[14] and is now 143 km (89 mi), set in open air experiments in the Canary Islands, done between the two astronomical observatories of the Instituto de Astrofísica de Canarias.[14] There has been a recent record set (as of September 2015) using superconducting nanowire detectors that reached the distance of 102 km (63 mi) over optical fiber.[15] For material systems, the record distance is 21 metres (69 ft).[16]

A variant of teleportation called "open-destination" teleportation, with receivers located at multiple locations, was demonstrated in 2004 using five-photon entanglement.[17] Teleportation of a composite state of two single qubits has also been realized.[18] In April 2011, experimenters reported that they had demonstrated teleportation of wave packets of light up to a bandwidth of 10 MHz while preserving strongly nonclassical superposition states.[19][20] In August 2013, the achievement of "fully deterministic" quantum teleportation, using a hybrid technique, was reported.[21] On 29 May 2014, scientists announced a reliable way of transferring data by quantum teleportation. Quantum teleportation of data had been done before but with highly unreliable methods.[22][23] On 26 February 2015, scientists at the University of Science and Technology of China in Hefei, led by Chao-yang Lu and Jian-Wei Pan carried out the first experiment teleporting multiple degrees of freedom of a quantum particle. They managed to teleport the quantum information from ensemble of rubidium atoms to another ensemble of rubidium atoms over a distance of 150 metres (490 ft) using entangled photons.[24][25][26] In 2016, researchers demonstrated quantum teleportation with two independent sources which are separated by 6.5 km (4.0 mi) in Hefei optical fiber network.[27] In September 2016, researchers at the University of Calgary demonstrated quantum teleportation over the Calgary metropolitan fiber network over a distance of 6.2 km (3.9 mi).[28] In December 2020, as part of the INQNET collaboration, researchers achieved quantum teleportation over a total distance of 44 km (27.3 mi) with fidelities exceeding 90%.[29][30]

Researchers have also successfully used quantum teleportation to transmit information between clouds of gas atoms, notable because the clouds of gas are macroscopic atomic ensembles.[31][32]

It is also possible to teleport *logical operations*, see quantum gate teleportation. In 2018, physicists at Yale demonstrated a deterministic teleported CNOT operation between logically encoded qubits.[33]

First proposed theoretically in 1993, quantum teleportation has since been demonstrated in many different guises. It has been carried out using two-level states of a single photon, a single atom and a trapped ion – among other quantum objects – and also using two photons. In 1997, two groups experimentally achieved quantum teleportation. The first group, led by Sandu Popescu, was based in Italy. An experimental group led by Anton Zeilinger followed a few months later.



Schematic of the quantum teleportation experiment performed by Zeilinger's group in 1997. For details, see the text.

The results obtained from experiments done by Popescu's group concluded that classical channels alone could not replicate the teleportation of linearly polarized state and an elliptically polarized state. The Bell state measurement distinguished between the four Bell states, which can allow for a 100% success rate of teleportation, in an ideal representation.[2]

Zeilinger's group produced a pair of entangled photons by implementing the process of parametric down-conversion. In order to ensure that the two photons cannot be distinguished by their arrival times, the photons were generated using a pulsed pump beam. The photons were then sent through narrow-bandwidth filters to produce a coherence time that is much longer than the length of the pump pulse. They then used a two-photon interferometry for analyzing the entanglement so that the quantum property could be recognized when it is transferred from one photon to the other.[3]

Photon 1 was polarized at 45° in the first experiment conducted by Zeilinger's group. Quantum teleportation is verified when both photons are detected in the $|\Psi^-\rangle_{12}$ state, which has a probability of 25%. Two detectors, f1 and f2, are placed behind the beam splitter, and recording the coincidence will identify the $|\Psi^-\rangle_{12}$ state. If there is a coincidence between detectors f1 and f2, then photon 3 is predicted to be polarized at a 45° angle. Photon 3 is passed through a polarizing beam splitter that selects +45° and −45° polarization. If quantum teleportation has happened, only detector d2, which is at the +45° output, will register a detection. Detector d1, located at the −45° output, will not detect a photon. If there is a coincidence between d2f1f2, with the 45° analysis, and a lack of a d1f1f2 coincidence, with −45° analysis, it is proof that the information from the polarized photon 1 has been teleported to photon 3 using quantum teleportation.[3]

Quantum teleportation over 143 km

Zeilinger's group developed an experiment using active feed-forward in real time and two free-space optical links, quantum and classical, between the Canary Islands of La Palma and Tenerife, a distance of over 143 kilometers. The results were published in 2012. In order to achieve teleportation, a frequency-uncorrelated polarization-entangled photon pair source, ultra-low-noise single-photon detectors and entanglement assisted clock synchronization were implemented. The two locations were entangled to share the auxiliary state:[14]

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}((|H\rangle_2|V\rangle_3) - (|V\rangle_2|H\rangle_3))$$

La Palma and Tenerife can be compared to the quantum characters Alice and Bob. Alice and Bob share the entangled state above, with photon 2 being with Alice and photon 3 being with Bob. A third party, Charlie, provides photon 1 (the input photon) which will be teleported to Alice in the generalized polarization state:

$$|\phi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1$$

where the complex numbers α and β are unknown to Alice or Bob.

Alice will perform a Bell-state measurement (BSM) that randomly projects the two photons onto one of the four Bell states with each one having a probability of 25%. Photon 3 will be projected onto $|\phi\rangle$, the input state. Alice transmits the outcome of the BSM to Bob, via the classical channel, where Bob is able to apply the corresponding unitary operation to obtain photon 3 in the initial state of photon 1. Bob will not have to do anything if he detects the $|\psi^-\rangle_{12}$ state. Bob will need to apply a π phase shift to photon 3 between the horizontal and vertical component if the $|\psi^+\rangle_{12}$ state is detected.[14]

The results of Zeilinger's group concluded that the average fidelity (overlap of the ideal teleported state with the measured density matrix) was 0.863 with a standard deviation of 0.038. The link attenuation during their experiments varied between 28.1 dB and 39.0 dB, which was a result of strong winds and rapid temperature changes. Despite the high loss in the quantum free-space channel, the average fidelity surpassed the classical limit of 2/3. Therefore, Zeilinger's group successfully demonstrated quantum teleportation over a distance of 143 km.[14]

Quantum teleportation across the Danube River

In 2004, a quantum teleportation experiment was conducted across the Danube River in Vienna, a total of 600 meters. An 800-meter-long optical fiber wire was installed in a public sewer system underneath the Danube River, and it was exposed to temperature changes and other environmental influences. Alice must perform a joint Bell state measurement (BSM) on photon b, the input photon, and photon c, her part of the entangled photon pair (photons c and d). Photon d, Bob's receiver photon, will contain all of the information on the input photon b, except for a phase rotation that depends on the state that Alice observed. This experiment implemented an active feed-forward system that sends Alice's measurement results via a classical microwave channel with a fast electro-optical modulator in order to exactly replicate Alice's input photon. The teleportation fidelity obtained from the linear polarization state at 45° varied between 0.84 and 0.90, which is well above the classical fidelity limit of 0.66.[12]

Deterministic quantum teleportation with atoms

Three qubits are required for this process: the source qubit from the sender, the ancillary qubit, and the receiver's target qubit, which is maximally entangled with the ancillary qubit. For this experiment, $^{40}Ca^+$ ions were used as the qubits. Ions 2 and 3 are prepared in the Bell state $|\psi^+\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2|1\rangle_3 + |1\rangle_2|0\rangle_3)$. The state of ion 1 is prepared arbitrarily. The quantum states of

ions 1 and 2 are measured by illuminating them with light at a specific wavelength. The obtained fidelities for this experiment ranged between 73% and 76%. This is larger than the maximum possible average fidelity of 66.7% that can be obtained using completely classical resources.[34]

Ground-to-satellite quantum teleportation

The quantum state being teleported in this experiment is $|\chi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1$, where α and β are unknown complex numbers, $|H\rangle$ represents the horizontal polarization state, and $|V\rangle$ represents the vertical polarization state. The qubit prepared in this state is generated in a laboratory in Ngari, Tibet. The goal was to teleport the quantum information of the qubit to the Micius satellite that was launched on August 16, 2016, at an altitude of around 500 km. When a Bell state measurement is conducted on photons 1 and 2 and the resulting state is $|\phi^+\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 + |V\rangle_1|V\rangle_2))$, photon 3 carries this desired state. If the Bell state detected is $|\phi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 - |V\rangle_1|V\rangle_2)$, then a phase shift of π is applied to the state to get the desired quantum state. The distance between the ground station and the satellite changes from as little as 500 km to as large as 1,400 km. Because of the changing distance, the channel loss of the uplink varies between 41 dB and 52 dB. The average fidelity obtained from this experiment was 0.80 with a standard deviation of 0.01. Therefore, this experiment successfully established a ground-to-satellite uplink over a distance of 500–1,400 km using quantum teleportation. This is an essential step towards creating a global-scale quantum internet.[6]

Formal presentation

There are a variety of ways in which the teleportation protocol can be written mathematically. Some are very compact but abstract, and some are verbose but straightforward and concrete. The presentation below is of the latter form: verbose, but has the benefit of showing each quantum state simply and directly. Later sections review more compact notations.

The teleportation protocol begins with a quantum state or qubit $|\psi\rangle$, in Alice's possession, that she wants to convey to Bob. This qubit can be written generally, in bra–ket notation, as:

$$|\psi\rangle_C = \alpha|0\rangle_C + \beta|1\rangle_C.$$

The subscript *C* above is used only to distinguish this state from *A* and *B*, below.

Next, the protocol requires that Alice and Bob share a maximally entangled state. This state is fixed in advance, by mutual agreement between Alice and Bob, and can be any one of the four Bell states shown. It does not matter which one.

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B),$$
$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B),$$
$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B).$$

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B),$$

In the following, assume that Alice and Bob share the state $|\Phi^+\rangle_{AB}$. Alice obtains one of the particles in the pair, with the other going to Bob. (This is implemented by preparing the particles together and shooting them to Alice and Bob from a common source.) The subscripts *A* and *B* in the entangled state refer to Alice's or Bob's particle.

At this point, Alice has two particles (*C*, the one she wants to teleport, and *A*, one of the entangled pair), and Bob has one particle, *B*. In the total system, the state of these three particles is given by

$$|\psi\rangle_C \otimes |\Phi^+\rangle_{AB} = (\alpha|0\rangle_C + \beta|1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B).$$

Alice will then make a local measurement in the Bell basis (i.e. the four Bell states) on the two particles in her possession. To make the result of her measurement clear, it is best to write the state of Alice's two qubits as superpositions of the Bell basis. This is done by using the following general identities, which are easily verified:

$$|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle),$$

$$|0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle),$$

$$|1\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle),$$

and

$$|1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle).$$

After expanding the expression for $|\psi\rangle_C \otimes |\Phi^+\rangle_{AB}$, one applies these identities to the qubits with *A* and *C* subscripts. In particular,

$$\alpha\frac{1}{\sqrt{2}}|0\rangle_C \otimes |0\rangle_A \otimes |0\rangle_B = \alpha\frac{1}{2}(|\Phi^+\rangle_{CA} + |\Phi^-\rangle_{CA}) \otimes |0\rangle_B,$$

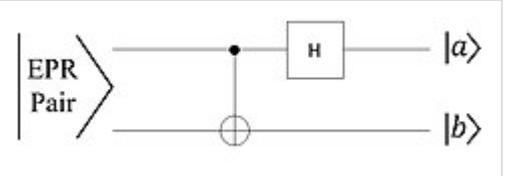
and the other terms follow similarly. Combining similar terms, the total three particle state of *A*, *B* and *C* together becomes the following four-term superposition:[35]

$$\begin{aligned}
&|\psi\rangle_C \otimes |\Phi^+\rangle_{AB} = \\
&\frac{1}{2}\Big[\,|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) \;+\; |\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B) \\
&+\; |\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) \;+\; |\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)\Big].
\end{aligned}$$

Note that all three particles are still in the same total state since no operations have been performed. Rather, the above is just a change of basis on Alice's part of the system. This change has moved the entanglement from particles A and B to particles C and A. The actual teleportation occurs when Alice measures her two qubits (C and A) in the Bell basis

$$|\Phi^+\rangle_{CA}, |\Phi^-\rangle_{CA}, |\Psi^+\rangle_{CA}, |\Psi^-\rangle_{CA}.$$

Equivalently, the measurement may be done in the computational basis, $\{|0\rangle, |1\rangle\}$, by mapping each Bell state uniquely to one of $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ with the quantum circuit in the figure to the right.



A simple quantum circuit that maps one of the four Bell states (the EPR pair in the picture) into one of the four two-qubit computational basis states. The circuit consists of a CNOT gate followed by a Hadamard operation. In the outputs, a and b take on values of 0 or 1.

The result of Alice's (local) measurement is a collection of two classical bits (00, 01, 10 or 11) related to one of the following four states (with equal probability of 1/4), after the three-particle state has collapsed into one of the states:

- $|\Phi^+\rangle_{CA} \otimes (\alpha|0\rangle_B + \beta|1\rangle_B)$
- $|\Phi^-\rangle_{CA} \otimes (\alpha|0\rangle_B - \beta|1\rangle_B)$
- $|\Psi^+\rangle_{CA} \otimes (\alpha|1\rangle_B + \beta|0\rangle_B)$
- $|\Psi^-\rangle_{CA} \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)$

Alice's two particles are now entangled to each other, in one of the four Bell states, and the entanglement originally shared between Alice's and Bob's particles is now broken. Bob's particle takes on one of the four superposition states shown above. Note how Bob's qubit is now in a state that resembles the state to be teleported. The four possible states for Bob's qubit are unitary images of the state to be teleported.

The result of Alice's Bell measurement tells her which of the above four states the system is in. She can now send her result to Bob through a classical channel. Two classical bits can communicate which of the four results she obtained. After Bob receives the message from Alice, he will know which of the four states his particle is in. Using this information, he performs a unitary operation on his particle to transform it to the desired state $\alpha|0\rangle_B + \beta|1\rangle_B$:

- If Alice indicates her result is $|\Phi^+\rangle_{CA}$, Bob knows his qubit is already in the desired state and does nothing. This amounts to the trivial unitary operation, the identity operator.
- If the message indicates $|\Phi^-\rangle_{CA}$, Bob would send his qubit through the unitary quantum gate given by the Pauli matrix

$$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

to recover the state.

- If Alice's message corresponds to $|\Psi^+\rangle_{CA}$, Bob applies the gate

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

to his qubit.

- Finally, for the remaining case, the appropriate gate is given by

$$\sigma_3\sigma_1 = -\sigma_1\sigma_3 = i\sigma_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Teleportation is thus achieved. The above-mentioned three gates correspond to rotations of π radians (180°) about appropriate axes (X, Y and Z) in the Bloch sphere picture of a qubit.

Some remarks:

- After this operation, Bob's qubit will take on the state $|\psi\rangle_B = \alpha|0\rangle_B + \beta|1\rangle_B$, and Alice's qubit becomes an (undefined) part of an entangled state. Teleportation does not result in the copying of qubits, and hence is consistent with the no-cloning theorem.
- There is no transfer of matter or energy involved. Alice's particle has not been physically moved to Bob; only its state has been transferred. The term "teleportation", coined by Bennett, Brassard, Crépeau, Jozsa, Peres and Wootters, reflects the indistinguishability of quantum mechanical particles.
- For every qubit teleported, Alice needs to send Bob two classical bits of information. These two classical bits do not carry complete information about the qubit being teleported. If an eavesdropper intercepts the two bits, she may know exactly what Bob needs to do in order to recover the desired state. However, this information is useless if she cannot interact with the entangled particle in Bob's possession.

Certifying quantum teleportation

When implementing the quantum teleportation protocol, different experimental noises may arise affecting the state transference.[36] The usual way to benchmark a particular teleportation procedure is by using the average fidelity: Given an arbitrary teleportation protocol producing output states ρ_i with probability p_i for an initial state $\rho = |\psi\rangle\langle\psi|$, the average fidelity is defined as:[37]

$$\langle\overline{F}\rangle = \int \sum_i p_i F(\rho, \rho_i) d\psi$$

where the integration is performed over the Haar measure defined by assuming maximal uncertainty over the initial quantum states $|\psi\rangle$, and $F(\rho, \rho_i) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\rho_i\sqrt{\rho}}\right)^2$ is the Uhlmann-Jozsa fidelity.

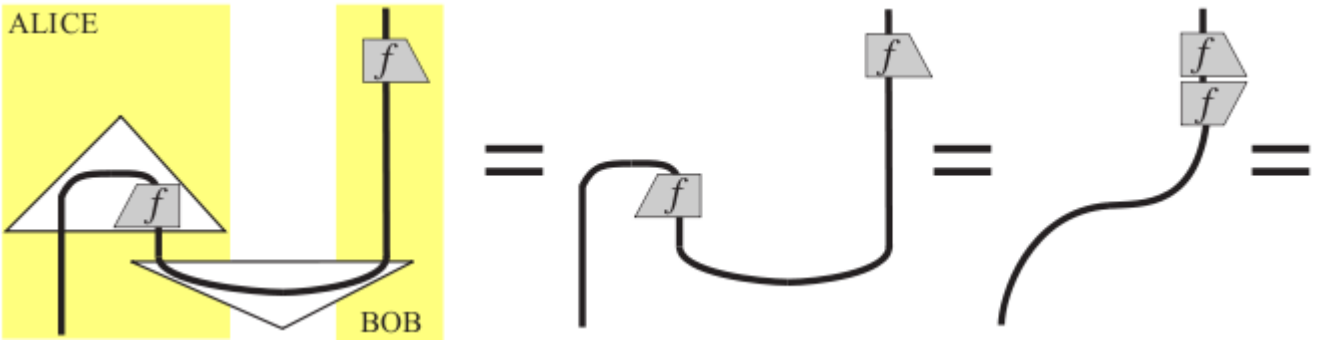
The widely known classical threshold is obtained by optimizing the average fidelity over all classical protocols (i.e. when the sender Alice and the receiver Bob can use just a classical channel to communicate with each other). When teleportation involves qubit states, the maximal classical average fidelity is $2/3$.[38][39] In this way, a particular protocol with average fidelity $\langle\overline{F}\rangle$ is certified as *useful* if $\langle\overline{F}\rangle \geq 2/3$.[6][12][14]

However, using the Uhlmann-Jozsa fidelity as the *unique* distance measure for benchmarking teleportation is not justified, and one may choose different distinguishability measures.[40] For example, there may exist reasons depending on the context in which other measures might be more suitable than fidelity.[41] In this way, the average distance of teleportation is defined as:[42]

$$\langle \overline{D} \rangle = \int \sum_i p_i D(\rho, \rho_i) d\psi$$

being $D(\rho, \sigma)$ a well-behaved (i.e. satisfying identity of indiscernibles and unitary invariance) distinguishability measure between quantum states. Consequently, different classical thresholds exist, depending on the considered distance measure (classical thresholds for Trace distance, quantum Jensen–Shannon divergence, transmission distance, Bures distance, wootters distance, and quantum Hellinger distance, among others, were obtained in Ref. [42]). This points out a particular issue when certifying quantum teleportation: Given a teleportation protocol, its certification is not a universal fact in the sense that depends on the distance used. Then, a particular protocol might be certified as useful for a set of distance quantifiers, and non-useful for other distinguishability measures.[42]

Alternative notations



Quantum teleportation in its diagrammatic form.[43] employing Penrose graphical notation.[44] Formally, such a computation takes place in a dagger compact category. This results in the abstract description of quantum teleportation as employed in categorical quantum mechanics.

There are a variety of different notations in use that describe the teleportation protocol. One common one is by using the notation of quantum gates.

In the above derivation, the unitary transformation that is the change of basis (from the standard product basis into the Bell basis) can be written using quantum gates. Direct calculation shows that this gate is given by

$$G = (H \otimes I)\,\mathrm{CNOT}$$

where H is the one qubit Walsh-Hadamard gate and CNOT is the Controlled NOT gate.

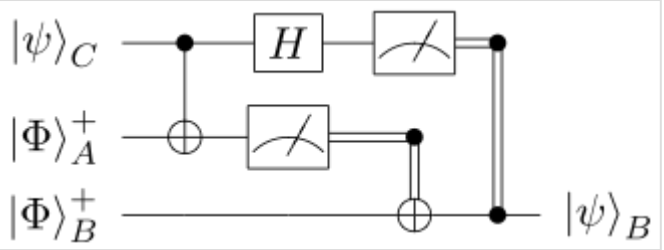
Entanglement swapping

Teleportation can be applied not just to pure states, but also mixed states, that can be regarded as the state of a single subsystem of an entangled pair. The so-called entanglement swapping is a simple and illustrative example.

If Alice and Bob share an entangled pair, and Bob teleports his particle to Carol, then Alice's particle is now entangled with Carol's particle. This situation can also be viewed symmetrically as follows:

Alice and Bob share an entangled pair, and Bob and Carol share a different entangled pair. Now let Bob perform a projective measurement on his two particles in the Bell basis and communicate the result to Carol. These actions are precisely the teleportation protocol described above with Bob's first particle, the one entangled with Alice's particle, as the state to be teleported. When Carol finishes the protocol she now has a particle with the teleported state, that is an entangled state with Alice's particle. Thus, although Alice and Carol never interacted with each other, their particles are now entangled.

A detailed diagrammatic derivation of entanglement swapping has been given by Bob Coecke,[47] presented in terms of categorical quantum mechanics.



Quantum circuit representation for teleportation of a quantum state,[45][46] as described above. The circuit consumes the $|\Phi^+\rangle$ Bell state and the qubit to teleport as input, and consists of CNOT, Hadamard, two measurements of two qubits, and finally, two gates with classical control: a Pauli X, and a Pauli Z, meaning that if the result from the measurement was $|1\rangle$, then the classically controlled Pauli gate is executed. After the circuit has run to completion, the value of $|\psi\rangle_C$ will have moved to, or *teleported* to $|\psi\rangle_B$, and $|\psi\rangle_C$ will have its value set to either $|0\rangle$ or $|1\rangle$, depending on the result from the measurement on that qubit.
This circuit can also be used for *entanglement swapping*, if $|\psi\rangle_C$ is one of the qubits that make up an entangled state, as described in the text.

Algorithm for swapping Bell pairs

An important application of entanglement swapping is distributing Bell states for use in entanglement distributed quantum networks. A technical description of the entanglement swapping protocol is given here for pure Bell states.

1. Alice and Bob locally prepare known Bell pairs resulting in the initial state:
   $|\psi\rangle_{\text{in}} = |\Phi^+\rangle_{A_1,A_2}|\Phi^+\rangle_{B_1,B_2}$
2. Alice sends qubit A_1 to a third party Carol
3. Bob sends qubit B_1 to Carol
4. Carol performs a Bell projection between A_1 and B_1 that by chance (all four Bell states are possible and recognizable) results in the measurement outcome:
   $\langle\Phi^+|_{A_1,B_1}|\psi\rangle_{\text{in}} = |\Phi^+\rangle_{A_2,B_2}$
5. In the case of the other three Bell projection outcomes, local corrections given by Pauli operators are made by Alice and or Bob after Carol has communicated the results of the measurement.
   $\langle\Phi^-|_{A_1,B_1}|\psi\rangle_{\text{in}} = \hat{Z}_{B_2}|\Phi^+\rangle_{A_2,B_2}$
   $\langle\Psi^+|_{A_1,B_1}|\psi\rangle_{\text{in}} = \hat{X}_{B_2}|\Phi^+\rangle_{A_2,B_2}$
   $\langle\Psi^-|_{A_1,B_1}|\psi\rangle_{\text{in}} = \hat{X}_{B_2}\hat{Z}_{B_2}|\Phi^+\rangle_{A_2,B_2}$
6. Alice and Bob now have a Bell pair between qubits A_2 and B_2
   $|\psi\rangle_{\text{out}} = |\Phi^+\rangle_{A_2,B_2}$

Generalizations of the teleportation protocol

The basic teleportation protocol for a qubit described above has been generalized in several directions, in particular regarding the dimension of the system teleported and the number of parties involved (either as sender, controller, or receiver).

d-dimensional systems

A generalization to d-level systems (so-called qudits) is straight forward and was already discussed in the original paper by Bennett *et al.*:[1] the maximally entangled state of two qubits has to be replaced by a maximally entangled state of two qudits and the Bell measurement by a measurement defined by a maximally entangled orthonormal basis. All possible such generalizations were discussed by Werner in 2001.[48]

The generalization to infinite-dimensional so-called continuous-variable systems was proposed by Braunstein and Kimble[49] and led to the first teleportation experiment that worked unconditionally.[50]

Multipartite versions

The use of multipartite entangled states instead of a bipartite maximally entangled state allows for several new features: either the sender can teleport information to several receivers either sending the same state to all of them (which allows to reduce the amount of entanglement needed for the process)[51] or teleporting multipartite states[52] or sending a single state in such a way that the receiving parties need to cooperate to extract the information.[53] A different way of viewing the latter setting is that some of the parties can control whether the others can teleport.

Logic gate teleportation

In general, mixed states ρ may be transported, and a linear transformation ω applied during teleportation, thus allowing data processing of quantum information. This is one of the foundational building blocks of quantum information processing. This is demonstrated below.

General description

A general teleportation scheme can be described as follows. Three quantum systems are involved. System 1 is the (unknown) state ρ to be teleported by Alice. Systems 2 and 3 are in a maximally entangled state ω that are distributed to Alice and Bob, respectively. The total system is then in the state

$$\rho \otimes \omega.$$

A successful teleportation process is a LOCC quantum channel Φ that satisfies

$$(\mathrm{Tr}_{12} \circ \Phi)(\rho \otimes \omega) = \rho,$$

where Tr_{12} is the partial trace operation with respect systems 1 and 2, and $\circ$ denotes the composition of maps. This describes the channel in the Schrödinger picture.

Taking adjoint maps in the Heisenberg picture, the success condition becomes

$$\langle \Phi(\rho \otimes \omega) | I \otimes O \rangle = \langle \rho | O \rangle$$

for all observable *O* on Bob's system. The tensor factor in $I \otimes O$ is $\mathbf{12} \otimes \mathbf{3}$ while that of $\rho \otimes \omega$ is $\mathbf{1} \otimes \mathbf{23}$.

Further details

The proposed channel Φ can be described more explicitly. To begin teleportation, Alice performs a local measurement on the two subsystems (1 and 2) in her possession. Assume the local measurement have *effects*

$$F_i = M_i^2.$$

If the measurement registers the *i*-th outcome, the overall state collapses to

$$(M_i \otimes I)(\rho \otimes \omega)(M_i \otimes I).$$

The tensor factor in $(M_i \otimes I)$ is $\mathbf{12} \otimes \mathbf{3}$ while that of $\rho \otimes \omega$ is $\mathbf{1} \otimes \mathbf{23}$. Bob then applies a corresponding local operation Ψ_i on system 3. On the combined system, this is described by

$$(Id \otimes \Psi_i)(M_i \otimes I)(\rho \otimes \omega)(M_i \otimes I).$$

where *Id* is the identity map on the composite system $\mathbf{1} \otimes \mathbf{2}$.

Therefore, the channel Φ is defined by

$$\Phi(\rho \otimes \omega) = \sum_i (Id \otimes \Psi_i)(M_i \otimes I)(\rho \otimes \omega)(M_i \otimes I)$$

Notice Φ satisfies the definition of LOCC. As stated above, the teleportation is said to be successful if, for all observable *O* on Bob's system, the equality

$$\langle \Phi(\rho \otimes \omega), I \otimes O \rangle = \langle \rho, O \rangle$$

holds. The left hand side of the equation is:

$$\sum_i \langle (Id \otimes \Psi_i)(M_i \otimes I)(\rho \otimes \omega)(M_i \otimes I),\ I \otimes O \rangle$$

$$= \sum_i \langle (M_i \otimes I)(\rho \otimes \omega)(M_i \otimes I),\ I \otimes \Psi_i^*(O) \rangle$$

where Ψ_i* is the adjoint of Ψ_i in the Heisenberg picture. Assuming all objects are finite dimensional, this becomes

$$\sum_i \mathbf{Tr}\ (\rho \otimes \omega)(F_i \otimes \Psi_i^*(O)).$$

The success criterion for teleportation has the expression

$$\sum_i \mathbf{Tr}\ (\rho \otimes \omega)(F_i \otimes \Psi_i^*(O)) = \mathbf{Tr}\ \rho \cdot O.$$

Local explanation of the phenomenon

A local explanation of quantum teleportation is put forward by David Deutsch and Patrick Hayden, with respect to the many-worlds interpretation of quantum mechanics. Their paper asserts that the two bits that Alice sends Bob contain "locally inaccessible information" resulting in the teleportation of the quantum state. "The ability of quantum information to flow through a classical channel [...], surviving decoherence, is [...] the basis of quantum teleportation."[54]

Recent developments

While quantum teleportation is in an infancy stage, there are many aspects pertaining to teleportation that scientists are working to better understand or improve the process that include:

Higher dimensions

Quantum teleportation can improve the errors associated with fault tolerant quantum computation via an arrangement of logic gates. Experiments by D. Gottesman and I. L. Chuang have determined that a "Clifford hierarchy"[55] gate arrangement which acts to enhance protection against environmental errors. Overall, a higher threshold of error is allowed with the Clifford hierarchy as the sequence of gates requires less resources that are needed for computation. While the more gates that are used in a quantum computer create more noise, the gates arrangement and use of teleportation in logic transfer can reduce this noise as it calls for less "traffic" that is compiled in these quantum networks.[56] The more qubits used for a quantum computer, the more levels are added to a gate arrangement, with the diagonalization of gate arrangement varying in degree. Higher dimension analysis involves the higher level gate arrangement of the Clifford hierarchy.[57]

Information quality

Considering the previously mentioned requirement of an intermediate entangled state for quantum teleportation, there needs to be consideration placed on to the purity of this state for information quality. A protection that has been developed involves the use of continuous variable information (rather than a typical discrete variable) creating a superimposed coherent intermediate state. This involves making a phase shift in the received information and then adding a mixing step upon reception using a preferred state, which could be an odd or even coherent state, that will be "conditioned to the classical information of the sender" creating a two mode state that contains the originally sent information.[58]

There have also been developments with teleporting information between systems that already have quantum information in them. Experiments done by Feng, Xu, Zhou et al. have demonstrated that teleportation of a qubit to a photon that already has a qubit worth of information is possible due to using

an optical qubit-ququart entangling gate.[4] This quality can increase computation possibilities as calculations can be done based on previously stored information allowing for improvements on past calculations.

See also

- Superdense coding
- Quantum complex network
- Quantum mechanics
  - Introduction to quantum mechanics
  - Quantum computer
  - Quantum cryptography
  - Quantum nonlocality
  - Heisenberg uncertainty principle
- Wheeler–Feynman absorber theory

References

Specific

1. Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K. (29 March 1993). "Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels" (https://doi.org/10.1103%2FPhysRevLett.70.1895). *Physical Review Letters*. **70** (13): 1895–1899. Bibcode:1993PhRvL..70.1895B (https://ui.adsabs.harvard.edu/abs/1993PhRvL..70.1895B). CiteSeerX 10.1.1.46.9405 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.46.9405). doi:10.1103/PhysRevLett.70.1895 (https://doi.org/10.1103%2FPhysRevLett.70.1895). PMID 10053414 (https://pubmed.ncbi.nlm.nih.gov/10053414).
2. Boschi, D.; Branca, S.; De Martini, F.; Hardy, L.; Popescu, S. (9 February 1998). "Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels". *Physical Review Letters*. **80** (6): 1121–1125. arXiv:quant-ph/9710013 (https://arxiv.org/abs/quant-ph/9710013). Bibcode:1998PhRvL..80.1121B (https://ui.adsabs.harvard.edu/abs/1998PhRvL..80.1121B). doi:10.1103/PhysRevLett.80.1121 (https://doi.org/10.1103%2FPhysRevLett.80.1121). S2CID 15020942 (https://api.semanticscholar.org/CorpusID:15020942).
3. Bouwmeester, Dik; Pan, Jian-Wei; Mattle, Klaus; Eibl, Manfred; Weinfurter, Harald; Zeilinger, Anton (1 December 1997). "Experimental quantum teleportation". *Nature*. **390** (6660): 575–579. arXiv:1901.11004 (https://arxiv.org/abs/1901.11004). Bibcode:1997Natur.390..575B (https://ui.adsabs.harvard.edu/abs/1997Natur.390..575B). doi:10.1038/37539 (https://doi.org/10.1038%2F37539). S2CID 4422887 (https://api.semanticscholar.org/CorpusID:4422887).
4. Tianfeng Feng; Qiao Xu; Linxiang Zhou; Maolin Luo; Wuhong Zhang; Xiaoqi Zhou (2022). "Quantum information transfer between a two-level and a four-level quantum systems". *Photonics Research*. **10** (12): 2854. arXiv:2009.09421 (https://arxiv.org/abs/2009.09421). doi:10.1364/PRJ.461283 (https://doi.org/10.1364%2FPRJ.461283). S2CID 247011044 (https://api.semanticscholar.org/CorpusID:247011044).
5. Chang, Kenneth (17 June 2004). "Scientists Teleport not Kirk but an Atom" (https://www.nytimes.com/2004/06/17/us/scientists-teleport-not-kirk-but-an-atom.html). *New York Times*.

6. Ren, Ji-Gang; Xu, Ping; Yong, Hai-Lin; Zhang, Liang; Liao, Sheng-Kai; Yin, Juan; Liu, Wei-Yue; Cai, Wen-Qi; Yang, Meng; Li, Li; Yang, Kui-Xing; Han, Xuan; Yao, Yong-Qiang; Li, Ji; Wu, Hai-Yan; Wan, Song; Liu, Lei; Liu, Ding-Quan; Kuang, Yao-Wu; He, Zhi-Ping; Shang, Peng; Guo, Cheng; Zheng, Ru-Hua; Tian, Kai; Zhu, Zhen-Cai; Liu, Nai-Le; Lu, Chao-Yang; Shu, Rong; Chen, Yu-Ao; Peng, Cheng-Zhi; Wang, Jian-Yu; Pan, Jian-Wei (7 September 2017). "Ground-to-satellite quantum teleportation". *Nature*. **549** (7670): 70–73. arXiv:1707.00934 (https://arxiv.org/abs/1707.00934). Bibcode:2017Natur.549...70R (https://ui.adsabs.harvard.edu/abs/2017Natur.549...70R). doi:10.1038/nature23675 (https://doi.org/10.1038%2Fnature23675). PMID 28825708 (https://pubmed.ncbi.nlm.nih.gov/28825708). S2CID 4468803 (https://api.semanticscholar.org/CorpusID:4468803).
7. Migdał, Piotr; Jankiewicz, Klementyna; Grabarz, Paweł; Decaroli, Chiara; Cochin, Philippe (2022). "Visualizing quantum mechanics in an interactive simulation - Virtual Lab by Quantum Flytrap". *Optical Engineering*. **61** (8): 081808. arXiv:2203.13300 (https://arxiv.org/abs/2203.13300). Bibcode:2022OptEn..61h1808M (https://ui.adsabs.harvard.edu/abs/2022OptEn..61h1808M). doi:10.1117/1.OE.61.8.081808 (https://doi.org/10.1117%2F1.OE.61.8.081808).
8. Barrett, M. D.; Chiaverini, J.; Schaetz, T.; Britton, J.; Itano, W. M.; Jost, J. D.; Knill, E.; Langer, C.; Leibfried, D.; Ozeri, R.; Wineland, D. J. (2004). "Deterministic quantum teleportation of atomic qubits". *Nature*. **429** (6993): 737–739. Bibcode:2004Natur.429..737B (https://ui.adsabs.harvard.edu/abs/2004Natur.429..737B). doi:10.1038/nature02608 (https://doi.org/10.1038%2Fnature02608). PMID 15201904 (https://pubmed.ncbi.nlm.nih.gov/15201904). S2CID 1608775 (https://api.semanticscholar.org/CorpusID:1608775).
9. S. Pirandola; J. Eisert; C. Weedbrook; A. Furusawa; S. L. Braunstein (2015). "Advances in quantum teleportation". *Nature Photonics*. **9** (10): 641–652. arXiv:1505.07831 (https://arxiv.org/abs/1505.07831). Bibcode:2015NaPho...9..641P (https://ui.adsabs.harvard.edu/abs/2015NaPho...9..641P). doi:10.1038/nphoton.2015.154 (https://doi.org/10.1038%2Fnphoton.2015.154). S2CID 15074330 (https://api.semanticscholar.org/CorpusID:15074330).
10. Lo Franco, Rosario; Compagno, Giuseppe (2018). "Indistinguishability of Elementary Systems as a Resource for Quantum Information Processing". *Physical Review Letters*. **120** (24): 240403. arXiv:1712.00706 (https://arxiv.org/abs/1712.00706). Bibcode:2018PhRvL.120x0403L (https://ui.adsabs.harvard.edu/abs/2018PhRvL.120x0403L). doi:10.1103/PhysRevLett.120.240403 (https://doi.org/10.1103%2FPhysRevLett.120.240403). PMID 29957003 (https://pubmed.ncbi.nlm.nih.gov/29957003). S2CID 49562954 (https://api.semanticscholar.org/CorpusID:49562954).
11. Sun, K.; Wang, Y.; Liu, Z.-H.; Xu, X.-Y.; Xu, J.-S.; Li, C.-F.; Guo, G.-C.; Castellini, A.; Nosrati, F.; Compagno, G.; Lo Franco, R. (2020). "Experimental quantum entanglement and teleportation by tuning remote spatial indistinguishability of independent photons". *Optics Letters*. **45** (23): 6410–6413. arXiv:2003.10659 (https://arxiv.org/abs/2003.10659). Bibcode:2020OptL...45.6410S (https://ui.adsabs.harvard.edu/abs/2020OptL...45.6410S). doi:10.1364/OL.401735 (https://doi.org/10.1364%2FOL.401735). hdl:10447/449875 (https://hdl.handle.net/10447%2F449875). PMID 33258824 (https://pubmed.ncbi.nlm.nih.gov/33258824). S2CID 227245593 (https://api.semanticscholar.org/CorpusID:227245593).
12. Ursin, Rupert; Jennewein, Thomas; Aspelmeyer, Markus; Kaltenbaek, Rainer; Lindenthal, Michael; Walther, Philip; Zeilinger, Anton (18 August 2004). "Quantum teleportation across the Danube" (https://doi.org/10.1038%2F430849a). *Nature*. **430** (7002): 849. Bibcode:2004Natur.430..849U (https://ui.adsabs.harvard.edu/abs/2004Natur.430..849U). doi:10.1038/430849a (https://doi.org/10.1038%2F430849a). PMID 15318210 (https://pubmed.ncbi.nlm.nih.gov/15318210). S2CID 4426035 (https://api.semanticscholar.org/CorpusID:4426035).

13. Jin, Xian-Min; Ren, Ji-Gang; Yang, Bin; Yi, Zhen-Huan; Zhou, Fei; Xu, Xiao-Fan; Wang, Shao-Kai; Yang, Dong; Hu, Yuan-Feng; Jiang, Shuo; Yang, Tao; Yin, Hao; Chen, Kai; Peng, Cheng-Zhi; Pan, Jian-Wei (16 May 2010). "Experimental free-space quantum teleportation". *Nature Photonics*. **4** (6): 376. Bibcode:2010NaPho...4..376J (https://ui.adsabs.harvard.edu/abs/2010NaPho...4..376J). doi:10.1038/nphoton.2010.87 (https://doi.org/10.1038%2Fnphoton.2010.87).
14. Ma, Xiao-Song; Herbst, Thomas; Scheidl, Thomas; Wang, Daqing; Kropatschek, Sebastian; Naylor, William; Wittmann, Bernhard; Mech, Alexandra; Kofler, Johannes; Anisimova, Elena; Makarov, Vadim; Jennewein, Thomas; Ursin, Rupert; Zeilinger, Anton (5 September 2012). "Quantum teleportation over 143 kilometres using active feed-forward". *Nature*. **489** (7415): 269–273. arXiv:1205.3909 (https://arxiv.org/abs/1205.3909). Bibcode:2012Natur.489..269M (https://ui.adsabs.harvard.edu/abs/2012Natur.489..269M). doi:10.1038/nature11472 (https://doi.org/10.1038%2Fnature11472). PMID 22951967 (https://pubmed.ncbi.nlm.nih.gov/22951967). S2CID 209109 (https://api.semanticscholar.org/CorpusID:209109).
15. Takesue, Hiroki; Dyer, Shellee D.; Stevens, Martin J.; Verma, Varun; Mirin, Richard P.; Sae Woo Nam (20 October 2015). "Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors". *Optica*. **2** (10): 832–835. arXiv:1510.00476 (https://arxiv.org/abs/1510.00476). Bibcode:2015Optic...2..832T (https://ui.adsabs.harvard.edu/abs/2015Optic...2..832T). doi:10.1364/OPTICA.2.000832 (https://doi.org/10.1364%2FOPTICA.2.000832). S2CID 55109707 (https://api.semanticscholar.org/CorpusID:55109707).
16. Nölleke, Christian; Neuzner, Andreas; Reiserer, Andreas; Hahn, Carolin; Rempe, Gerhard; Ritter, Stephan (2013). "Efficient Teleportation between Remote Single-Atom Quantum Memories". *Physical Review Letters*. **110** (14): 140403. arXiv:1212.3127 (https://arxiv.org/abs/1212.3127). Bibcode:2013PhRvL.110n0403N (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110n0403N). doi:10.1103/PhysRevLett.110.140403 (https://doi.org/10.1103%2FPhysRevLett.110.140403). PMID 25166964 (https://pubmed.ncbi.nlm.nih.gov/25166964). S2CID 6597459 (https://api.semanticscholar.org/CorpusID:6597459).
17. Zhao, Zhi; Chen, Yu-Ao; Zhang, An-Ning; Yang, Tao; Briegel, Hans J.; Pan, Jian-Wei (2004). "Experimental demonstration of five-photon entanglement and open-destination teleportation". *Nature*. **430** (6995): 54–58. arXiv:quant-ph/0402096 (https://arxiv.org/abs/quant-ph/0402096). Bibcode:2004Natur.430...54Z (https://ui.adsabs.harvard.edu/abs/2004Natur.430...54Z). doi:10.1038/nature02643 (https://doi.org/10.1038%2Fnature02643). PMID 15229594 (https://pubmed.ncbi.nlm.nih.gov/15229594). S2CID 4336020 (https://api.semanticscholar.org/CorpusID:4336020).
18. Zhang, Qiang; Goebel, Alexander; Wagenknecht, Claudia; Chen, Yu-Ao; Zhao, Bo; Yang, Tao; Mair, Alois; Schmiedmayer, Jörg; Pan, Jian-Wei (2006). "Experimental quantum teleportation of a two-qubit composite system". *Nature Physics*. **2** (10): 678–682. arXiv:quant-ph/0609129 (https://arxiv.org/abs/quant-ph/0609129). Bibcode:2006NatPh...2..678Z (https://ui.adsabs.harvard.edu/abs/2006NatPh...2..678Z). doi:10.1038/nphys417 (https://doi.org/10.1038%2Fnphys417). S2CID 18201599 (https://api.semanticscholar.org/CorpusID:18201599).
19. Lee, Noriyuki; Hugo Benichi; Yuishi Takeno; Shuntaro Takeda; James Webb; Elanor Huntington; Akira Furusawa (April 2011). "Teleportation of Nonclassical Wave Packets of Light". *Science*. **332** (6027): 330–333. arXiv:1205.6253 (https://arxiv.org/abs/1205.6253). Bibcode:2011Sci...332..330L (https://ui.adsabs.harvard.edu/abs/2011Sci...332..330L). CiteSeerX 10.1.1.759.1059 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.759.1059). doi:10.1126/science.1201034 (https://doi.org/10.1126%2Fscience.1201034). PMID 21493853 (https://pubmed.ncbi.nlm.nih.gov/21493853). S2CID 206531447 (https://api.semanticscholar.org/CorpusID:206531447).
20. Trute, Peter. "Quantum teleporter breakthrough" (https://web.archive.org/web/20110418200747/http://www.unsw.edu.au/news/pad/articles/2011/apr/Quantum_teleport_paper.html). The University Of New South Wales. Archived from the original (http://www.unsw.edu.au/news/pad/articles/2011/apr/Quantum_teleport_paper.html) on 2011-04-18. Retrieved 2011-04-17.

21. Takeda, Shuntaro; Mizuta, Takahiro; Fuwa, Maria; van Loock, Peter; Furusawa, Akira (14 August 2013). "Deterministic quantum teleportation of photonic quantum bits by a hybrid technique". *Nature*. **500** (7462): 315–318. arXiv:1402.4895 (https://arxiv.org/abs/1402.4895). Bibcode:2013Natur.500..315T (https://ui.adsabs.harvard.edu/abs/2013Natur.500..315T). doi:10.1038/nature12366 (https://doi.org/10.1038%2Fnature12366). PMID 23955230 (https://pubmed.ncbi.nlm.nih.gov/23955230). S2CID 4344887 (https://api.semanticscholar.org/CorpusID:4344887).
22. Markoff, John (29 May 2014). "Scientists Report Finding Reliable Way to Teleport Data" (https://www.nytimes.com/2014/05/30/science/scientists-report-finding-reliable-way-to-teleport-data.html). *The New York Times*. Retrieved 2014-05-29.
23. Pfaff W, Hensen BJ, Bernien H, van Dam SB, Blok MS, Taminiau TH, Tiggelman MJ, Schouten RN, Markham M, Twitchen DJ, Hanson R (29 May 2014). "Unconditional quantum teleportation between distant solid-state quantum bits". *Science*. **345** (6196): 532–535. arXiv:1404.4369 (https://arxiv.org/abs/1404.4369). Bibcode:2014Sci...345..532P (https://ui.adsabs.harvard.edu/abs/2014Sci...345..532P). doi:10.1126/science.1253512 (https://doi.org/10.1126%2Fscience.1253512). PMID 25082696 (https://pubmed.ncbi.nlm.nih.gov/25082696). S2CID 2190249 (https://api.semanticscholar.org/CorpusID:2190249).
24. Commissariat, Tushna (27 February 2015). "Two quantum properties teleported together for first time" (http://physicsworld.com/cws/article/news/2015/feb/27/two-quantum-properties-teleported-together-for-first-time). *PhysicsWorld.com*.
25. Xi-Lin Wang; Xin-Dong Cai; Zu-En Su; Ming-Cheng Chen; Dian Wu; Li Li; Nai-Le Liu; Chao-Yang Lu; Jian-Wei Pan (26 February 2015). "Quantum teleportation of multiple degrees of freedom of a single photon". *Nature*. **518** (7540): 516–519. Bibcode:2015Natur.518..516W (https://ui.adsabs.harvard.edu/abs/2015Natur.518..516W). doi:10.1038/nature14246 (https://doi.org/10.1038%2Fnature14246). PMID 25719668 (https://pubmed.ncbi.nlm.nih.gov/25719668). S2CID 4448594 (https://api.semanticscholar.org/CorpusID:4448594).
26. Xia, Xiu-Xiu; Qi-Chao Sun; Qiang Zhang; Jian-Wei Pan (2018). "Long distance quantum teleportation". *Quantum Science and Technology*. **3** (1). 014012. Bibcode:2018QS&T....3a4012X (https://ui.adsabs.harvard.edu/abs/2018QS&T....3a4012X). doi:10.1088/2058-9565/aa9baf (https://doi.org/10.1088%2F2058-9565%2Faa9baf). S2CID 125240574 (https://api.semanticscholar.org/CorpusID:125240574).
27. Sun, Qi-Chao; Mao, Ya-Li; Chen, Sijing; Zhang, Wei; Jiang, Yang-Fan; Zhang, Yanbao; Zhang, Weijun; Miki, Shigehito; Yamashita, Taro; Terai, Hirotaka; Jiang, Xiao; Chen, Teng-Yun; You, Lixing; Chen, Xianfeng; Wang, Zhen; Fan, Jingyun; Zhang, Qiang; Pan, Jian-Wei (19 September 2016). "Quantum teleportation with independent sources and prior entanglement distribution over a network". *Nature Photonics*. **10** (10): 671–675. arXiv:1602.07081 (https://arxiv.org/abs/1602.07081). Bibcode:2016NaPho..10..671S (https://ui.adsabs.harvard.edu/abs/2016NaPho..10..671S). doi:10.1038/nphoton.2016.179 (https://doi.org/10.1038%2Fnphoton.2016.179). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893). S2CID 126228648 (https://api.semanticscholar.org/CorpusID:126228648).
28. Valivarthi, Raju; Puigibert, Marcel.li Grimau; Zhou, Qiang; Aguilar, Gabriel H.; Verma, Varun B.; Marsili, Francesco; Shaw, Matthew D.; Nam, Sae Woo; Oblak, Daniel (19 September 2016). "Quantum teleportation across a metropolitan fibre network". *Nature Photonics*. **10** (10): 676–680. arXiv:1605.08814 (https://arxiv.org/abs/1605.08814). Bibcode:2016NaPho..10..676V (https://ui.adsabs.harvard.edu/abs/2016NaPho..10..676V). doi:10.1038/nphoton.2016.180 (https://doi.org/10.1038%2Fnphoton.2016.180). ISSN 1749-4885 (https://search.worldcat.org/issn/1749-4885). S2CID 119163338 (https://api.semanticscholar.org/CorpusID:119163338).

29. Valivarthi, Raju; Davis, Samantha I.; Peña, Cristián; Xie, Si; Lauk, Nikolai; Narváez, Lautaro; Allmaras, Jason P.; Beyer, Andrew D.; Gim, Yewon; Hussein, Meraj; Iskander, George (4 December 2020). "Teleportation Systems Toward a Quantum Internet". *PRX Quantum*. **1** (2): 020317. arXiv:2007.11157 (https://arxiv.org/abs/2007.11157). Bibcode:2020PRXQ....1b0317V (https://ui.adsabs.harvard.edu/abs/2020PRXQ....1b0317V). doi:10.1103/PRXQuantum.1.020317 (https://doi.org/10.1103%2FPRXQuantum.1.020317). ISSN 2691-3399 (https://search.worldcat.org/issn/2691-3399). S2CID 220686903 (https://api.semanticscholar.org/CorpusID:220686903).
30. Tangermann, Victor (18 December 2020). "Researchers Achieve First "Sustained" Long Distance Quantum Teleportation" (https://futurism.com/researchers-achieve-first-sustained-long-distance-quantum-teleportation). *Futurism*. Retrieved 2021-06-06.
31. University of Copenhagen (13 June 2013). "Quantum teleportation between atomic systems over long distances" (http://phys.org/news/2013-06-quantum-teleportation-atomic-distances.html). *Phys.Org*.
32. Krauter, H.; Salart, D.; Muschik, C. A.; Petersen, J. M.; Shen, Heng; Fernholz, T.; Polzik, E. S. (2 June 2013). "Deterministic quantum teleportation between distant atomic objects". *Nature Physics*. **9** (7): 400. arXiv:1212.6746 (https://arxiv.org/abs/1212.6746). Bibcode:2013NatPh...9..400K (https://ui.adsabs.harvard.edu/abs/2013NatPh...9..400K). doi:10.1038/nphys2631 (https://doi.org/10.1038%2Fnphys2631). S2CID 118724313 (https://api.semanticscholar.org/CorpusID:118724313).
33. Chou, Kevin S.; Blumoff, Jacob Z.; Wang, Christopher S.; Reinhold, Philip C.; Axline, Christopher J.; Gao, Yvonne Y.; Frunzio, L.; Devoret, M. H.; Jiang, Liang; Schoelkopf, R. J. (2018). "Deterministic teleportation of a quantum gate between two logical qubits". *Nature*. **561** (7723): 368–373. arXiv:1801.05283 (https://arxiv.org/abs/1801.05283). Bibcode:2018Natur.561..368C (https://ui.adsabs.harvard.edu/abs/2018Natur.561..368C). doi:10.1038/s41586-018-0470-y (https://doi.org/10.1038%2Fs41586-018-0470-y). PMID 30185908 (https://pubmed.ncbi.nlm.nih.gov/30185908). S2CID 3820071 (https://api.semanticscholar.org/CorpusID:3820071).
34. Riebe, M.; Häffner, H.; Roos, C. F.; Hänsel, W.; Benhelm, J.; Lancaster, G. P. T.; Körber, T. W.; Becher, C.; Schmidt-Kaler, F.; James, D. F. V.; Blatt, R. (June 2004). "Deterministic quantum teleportation with atoms". *Nature*. **429** (6993): 734–737. Bibcode:2004Natur.429..734R (https://ui.adsabs.harvard.edu/abs/2004Natur.429..734R). doi:10.1038/nature02570 (https://doi.org/10.1038%2Fnature02570). PMID 15201903 (https://pubmed.ncbi.nlm.nih.gov/15201903). S2CID 4397716 (https://api.semanticscholar.org/CorpusID:4397716).
35. Nielsen, Michael A.; Chuang, Isaac (2010). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. pp. 26–27. ISBN 978-1-10700-217-3. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
36. Knoll, Laura T.; Schmiegelow, Christian T.; Larotonda, Miguel A. (28 October 2014). "Noisy quantum teleportation: An experimental study on the influence of local environments" (https://link.aps.org/doi/10.1103/PhysRevA.90.042332). *Physical Review A*. **90** (4): 042332. arXiv:1410.5771 (https://arxiv.org/abs/1410.5771). Bibcode:2014PhRvA..90d2332K (https://ui.adsabs.harvard.edu/abs/2014PhRvA..90d2332K). doi:10.1103/PhysRevA.90.042332 (https://doi.org/10.1103%2FPhysRevA.90.042332). hdl:11336/29814 (https://hdl.handle.net/11336%2F29814).
37. Pirandola, S.; Eisert, J.; Weedbrook, C.; Furusawa, A.; Braunstein, S. L. (October 2015). "Advances in quantum teleportation" (https://www.nature.com/articles/nphoton.2015.154). *Nature Photonics*. **9** (10): 641–652. arXiv:1505.07831 (https://arxiv.org/abs/1505.07831). Bibcode:2015NaPho...9..641P (https://ui.adsabs.harvard.edu/abs/2015NaPho...9..641P). doi:10.1038/nphoton.2015.154 (https://doi.org/10.1038%2Fnphoton.2015.154). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893).

38. Massar, S.; Popescu, S. (20 February 1995). "Optimal Extraction of Information from Finite Quantum Ensembles" (https://link.aps.org/doi/10.1103/PhysRevLett.74.1259). *Physical Review Letters*. **74** (8): 1259–1263. Bibcode:1995PhRvL..74.1259M (https://ui.adsabs.harvard.edu/abs/1995PhRvL..74.1259M). doi:10.1103/PhysRevLett.74.1259 (https://doi.org/10.1103%2FPhysRevLett.74.1259). PMID 10058975 (https://pubmed.ncbi.nlm.nih.gov/10058975).
39. Vidal, G.; Latorre, J. I.; Pascual, P.; Tarrach, R. (1 July 1999). "Optimal minimal measurements of mixed states" (https://dx.doi.org/10.1103/physreva.60.126). *Physical Review A*. **60** (1): 126–135. arXiv:quant-ph/9812068 (https://arxiv.org/abs/quant-ph/9812068). Bibcode:1999PhRvA..60..126V (https://ui.adsabs.harvard.edu/abs/1999PhRvA..60..126V). doi:10.1103/physreva.60.126 (https://doi.org/10.1103%2Fphysreva.60.126). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947).
40. Popescu, Sandu (7 February 1994). "Bell's inequalities versus teleportation: What is nonlocality?" (https://link.aps.org/doi/10.1103/PhysRevLett.72.797). *Physical Review Letters*. **72** (6): 797–799. Bibcode:1994PhRvL..72..797P (https://ui.adsabs.harvard.edu/abs/1994PhRvL..72..797P). doi:10.1103/PhysRevLett.72.797 (https://doi.org/10.1103%2FPhysRevLett.72.797). PMID 10056537 (https://pubmed.ncbi.nlm.nih.gov/10056537).
41. Ribeiro, G. A. P.; Rigolin, Gustavo (14 June 2024). "Finite-temperature detection of quantum critical points: A comparative study" (https://link.aps.org/doi/10.1103/PhysRevB.109.245122). *Physical Review B*. **109** (24): 245122. arXiv:2406.10178 (https://arxiv.org/abs/2406.10178). Bibcode:2024PhRvB.109x5122R (https://ui.adsabs.harvard.edu/abs/2024PhRvB.109x5122R). doi:10.1103/PhysRevB.109.245122 (https://doi.org/10.1103%2FPhysRevB.109.245122).
42. Bussandri, D. G.; Bosyk, G. M.; Toscano, F. (22 March 2024). "Challenges in certifying quantum teleportation: Moving beyond the conventional fidelity benchmark" (https://link.aps.org/doi/10.1103/PhysRevA.109.032618). *Physical Review A*. **109** (3): 032618. arXiv:2403.07994 (https://arxiv.org/abs/2403.07994). Bibcode:2024PhRvA.109c2618B (https://ui.adsabs.harvard.edu/abs/2024PhRvA.109c2618B). doi:10.1103/PhysRevA.109.032618 (https://doi.org/10.1103%2FPhysRevA.109.032618).
43. Coecke, Bob (2009). "Quantum Picturalism". *Contemporary Physics*. **51** (2010): 59–83. arXiv:0908.1787 (https://arxiv.org/abs/0908.1787). Bibcode:2010ConPh..51...59C (https://ui.adsabs.harvard.edu/abs/2010ConPh..51...59C). doi:10.1080/00107510903257624 (https://doi.org/10.1080%2F00107510903257624). S2CID 752173 (https://api.semanticscholar.org/CorpusID:752173).
44. R. Penrose, Applications of negative dimensional tensors, In: Combinatorial Mathematics and its Applications, D.~Welsh (Ed), pages 221–244. Academic Press (1971).
45. Colin P. Williams (2010). *Explorations in Quantum Computing*. Springer. pp. 496–499. ISBN 978-1-4471-6801-0.
46. Nielsen, Michael A.; Chuang, Isaac (2010). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. pp. 26–28. ISBN 978-1-10700-217-3. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
47. Coecke, Bob (2004). The logic of entanglement (Preprint). arXiv:quant-ph/0402014 (https://arxiv.org/abs/quant-ph/0402014).
48. Werner, Reinhard F. (2001). "All teleportation and dense coding schemes". *J. Phys. A: Math. Gen*. **34** (35): 7081–7094. arXiv:quant-ph/0003070 (https://arxiv.org/abs/quant-ph/0003070). Bibcode:2001JPhA...34.7081W (https://ui.adsabs.harvard.edu/abs/2001JPhA...34.7081W). doi:10.1088/0305-4470/34/35/332 (https://doi.org/10.1088%2F0305-4470%2F34%2F35%2F332). S2CID 9684671 (https://api.semanticscholar.org/CorpusID:9684671).
49. Braunstein, Samuel L.; Kimble, H. J. (26 January 1998). "Teleportation of Continuous Quantum Variables" (https://resolver.caltech.edu/CaltechAUTHORS:BRAprl98). *Physical Review Letters*. **80** (4): 869–872. Bibcode:1998PhRvL..80..869B (https://ui.adsabs.harvard.edu/abs/1998PhRvL..80..869B). doi:10.1103/PhysRevLett.80.869 (https://doi.org/10.1103%2FPhysRevLett.80.869).

50. Furusawa, A.; Sørensen, J. L.; Braunstein, S. L.; Fuchs, C. A.; Kimble, H. J.; Polzik, E. S. (1998). "Unconditional Quantum Teleportation". *Science*. **282** (5389): 706–709. Bibcode:1998Sci...282..706F (https://ui.adsabs.harvard.edu/abs/1998Sci...282..706F). doi:10.1126/science.282.5389.706 (https://doi.org/10.1126%2Fscience.282.5389.706). PMID 9784123 (https://pubmed.ncbi.nlm.nih.gov/9784123). S2CID 14269209 (https://api.semanticscholar.org/CorpusID:14269209).
51. W. Dür and J. I. Cirac (2000). "Multiparty teleportation". *J. Mod. Opt*. **47** (2–3): 247–255. Bibcode:2000JMOp...47..247D (https://ui.adsabs.harvard.edu/abs/2000JMOp...47..247D). doi:10.1080/09500340008244039 (https://doi.org/10.1080%2F09500340008244039). S2CID 216116503 (https://api.semanticscholar.org/CorpusID:216116503).
52. Yeo, Ye; Chua, Wee Kang (2006). "Teleportation and Dense Coding with Genuine Multipartite Entanglement". *Phys. Rev. Lett*. **96** (6): 060502. arXiv:quant-ph/0510029 (https://arxiv.org/abs/quant-ph/0510029). Bibcode:2006PhRvL..96f0502Y (https://ui.adsabs.harvard.edu/abs/2006PhRvL..96f0502Y). doi:10.1103/PhysRevLett.96.060502 (https://doi.org/10.1103%2FPhysRevLett.96.060502). PMID 16605974 (https://pubmed.ncbi.nlm.nih.gov/16605974). S2CID 5170837 (https://api.semanticscholar.org/CorpusID:5170837).
53. Karlsson, Anders; Bourennane, Mohamed (1998). "Quantum teleportation using three-particle entanglement". *Phys. Rev. A*. **58** (6): 4394–4400. Bibcode:1998PhRvA..58.4394K (https://ui.adsabs.harvard.edu/abs/1998PhRvA..58.4394K). doi:10.1103/PhysRevA.58.4394 (https://doi.org/10.1103%2FPhysRevA.58.4394).
54. Deutsch, David; Hayden, Patrick (1999). "Information Flow in Entangled Quantum Systems". *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. **456** (1999): 1759–1774. arXiv:quant-ph/9906007 (https://arxiv.org/abs/quant-ph/9906007). Bibcode:2000RSPSA.456.1759D (https://ui.adsabs.harvard.edu/abs/2000RSPSA.456.1759D). doi:10.1098/rspa.2000.0585 (https://doi.org/10.1098%2Frspa.2000.0585). S2CID 13998168 (https://api.semanticscholar.org/CorpusID:13998168).
55. Gottesman, Daniel; Chuang, Isaac L. (November 1999). "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". *Nature*. **402** (6760): 390–393. arXiv:quant-ph/9908010 (https://arxiv.org/abs/quant-ph/9908010). Bibcode:1999Natur.402..390G (https://ui.adsabs.harvard.edu/abs/1999Natur.402..390G). doi:10.1038/46503 (https://doi.org/10.1038%2F46503). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). S2CID 4411647 (https://api.semanticscholar.org/CorpusID:4411647).
56. Luo, Yi-Han; Chen, Ming-cheng; Erhard, Manuel; Zhong, Han-Sen; Wu, Dian; Tang, Hao-Yang; Zhao, Qi; Wang, Xi-Lin; Fujii, Keisuke; Li, Li; Liu, Nai-Le; Nemoto, Kae; Munro, William; Lu, Chao-Yang; Zeilinger, Anton; Pan, Jian-Wei (7 September 2020). "Quantum teleportation of physical qubits into logical code-spaces" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8433538). *PNAS*. **118** (36). e2026250118. arXiv:2009.06242 (https://arxiv.org/abs/2009.06242). doi:10.1073/pnas.2026250118 (https://doi.org/10.1073%2Fpnas.2026250118). PMC 8433538 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8433538). PMID 34479998 (https://pubmed.ncbi.nlm.nih.gov/34479998).
57. Nadish de Silva (2021). "Efficient quantum gate teleportation in higher dimensions". *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. **477** (2251). arXiv:2011.00127 (https://arxiv.org/abs/2011.00127). Bibcode:2021RSPSA.47700865D (https://ui.adsabs.harvard.edu/abs/2021RSPSA.477008650). doi:10.1098/rspa.2020.0865 (https://doi.org/10.1098%2Frspa.2020.0865). S2CID 226227346 (https://api.semanticscholar.org/CorpusID:226227346).
58. Pandey, Ravi; Prakash, Ranjana; Prakash, Hari (27 September 2021). "High success standard quantum teleportation using entangled coherent state and two-level atoms in cavities". *Quantum Inf Process*. **20** (10). 322. arXiv:2010.06829 (https://arxiv.org/abs/2010.06829). Bibcode:2021QuIP...20..322P (https://ui.adsabs.harvard.edu/abs/2021QuIP...20..322P). doi:10.1007/s11128-021-03264-0 (https://doi.org/10.1007%2Fs11128-021-03264-0). S2CID 222341312 (https://api.semanticscholar.org/CorpusID:222341312).

General

- Review on theory and experiments:
  - Pirandola, S.; Eisert, J.; Weedbrook, C.; Furusawa, A.; Braunstein, S. L. (2015). "Advances in Quantum Teleportation". *Nature Photonics*. **9** (10): 641–652. arXiv:1505.07831 (https://arxiv.org/abs/1505.07831). Bibcode:2015NaPho...9..641P (https://ui.adsabs.harvard.edu/abs/2015NaPho...9..641P). doi:10.1038/nphoton.2015.154 (https://doi.org/10.1038%2Fnphoton.2015.154). S2CID 15074330 (https://api.semanticscholar.org/CorpusID:15074330).
- Theoretical proposal:
  - Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K. (29 March 1993). "Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels". *Phys. Rev. Lett*. **70** (13): 1895–1899. Bibcode:1993PhRvL..70.1895B (https://ui.adsabs.harvard.edu/abs/1993PhRvL..70.1895B). doi:10.1103/PhysRevLett.70.1895 (https://doi.org/10.1103%2FPhysRevLett.70.1895). PMID 10053414 (https://pubmed.ncbi.nlm.nih.gov/10053414). S2CID 6599630 (https://api.semanticscholar.org/CorpusID:6599630). This is the seminal paper that laid out the entanglement protocol.
  - Vaidman, L. (February 1994). "Teleportation of Quantum States". *Phys. Rev. A*. **49** (2): 1473–1476. arXiv:hep-th/9305062 (https://arxiv.org/abs/hep-th/9305062). Bibcode:1994PhRvA..49.1473V (https://ui.adsabs.harvard.edu/abs/1994PhRvA..49.1473V). doi:10.1103/physreva.49.1473 (https://doi.org/10.1103%2Fphysreva.49.1473). PMID 9910380 (https://pubmed.ncbi.nlm.nih.gov/9910380). S2CID 8356637 (https://api.semanticscholar.org/CorpusID:8356637).
  - Shahriar, M.S.; Pradhan, P.; Gopal, V.; Morzinski, J.; Cardoso, G.; Pati, G.S. (2006). "Wavelength locking via teleportation using distant quantum entanglement and Bloch–Siegert oscillation". *Optics Communications*. **266** (1): 349–353. Bibcode:2006OptCo.266..349S (https://ui.adsabs.harvard.edu/abs/2006OptCo.266..349S). doi:10.1016/j.optcom.2006.04.072 (https://doi.org/10.1016%2Fj.optcom.2006.04.072).
  - Brassard, G; Braunstein, S; Cleve, R (1998). "Teleportation as a Quantum Computation". *Physica D*. **120** (1–2): 43–47. arXiv:quant-ph/9605035 (https://arxiv.org/abs/quant-ph/9605035). Bibcode:1998PhyD..120...43B (https://ui.adsabs.harvard.edu/abs/1998PhyD..120...43B). doi:10.1016/s0167-2789(98)00043-8 (https://doi.org/10.1016%2Fs0167-2789%2898%2900043-8). S2CID 15178313 (https://api.semanticscholar.org/CorpusID:15178313).
  - Peres, Asher (2003). "What is actually teleported?". arXiv:quant-ph/0304158 (https://arxiv.org/abs/quant-ph/0304158).
  - Rigolin, Gustavo (2005). "Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement". *Physical Review A*. **71** (3): 032303. arXiv:quant-ph/0407219 (https://arxiv.org/abs/quant-ph/0407219). Bibcode:2005PhRvA..71c2303R (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71c2303R). doi:10.1103/PhysRevA.71.032303 (https://doi.org/10.1103%2FPhysRevA.71.032303). S2CID 53941971 (https://api.semanticscholar.org/CorpusID:53941971).
  - Shi-Biao Zheng (2004) "Scheme for approximate conditional teleportation of an unknown atomic state without the Bell-state measurement", Phys. Rev. A **69**, 064302
  - Cardoso, Wesley B.; Avelar, A. T.; Baseia, B.; De Almeida, N. G. (2005). "Teleportation of entangled states without Bell-state measurement". *Physical Review A*. **72** (4). 045802. arXiv:quant-ph/0604156 (https://arxiv.org/abs/quant-ph/0604156). Bibcode:2005PhRvA..72d5802C (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72d5802C). doi:10.1103/PhysRevA.72.045802 (https://doi.org/10.1103%2FPhysRevA.72.045802). S2CID 11270460 (https://api.semanticscholar.org/CorpusID:11270460).

    - Leuenberger, Michael N.; Flatté, Michael E.; Awschalom, D. D. (2005). "Teleportation of Electronic Many-Qubit States Encoded in the Electron Spin of Quantum Dots via Single Photons". *Physical Review Letters*. **94** (10). 107401. Bibcode:2005PhRvL..94j7401L (https://ui.adsabs.harvard.edu/abs/2005PhRvL..94j7401L). doi:10.1103/PhysRevLett.94.107401 (https://doi.org/10.1103%2FPhysRevLett.94.107401). PMID 15783519 (https://pubmed.ncbi.nlm.nih.gov/15783519). S2CID 26932056 (https://api.semanticscholar.org/CorpusID:26932056).
    - Pyrkov, Alexey N.; Byrnes, Tim (2014). "Quantum teleportation of spin coherent states: Beyond continuous variables teleportation". *New Journal of Physics*. **16** (7). 073038. arXiv:1305.2479 (https://arxiv.org/abs/1305.2479). Bibcode:2014NJPh...16g3038P (https://ui.adsabs.harvard.edu/abs/2014NJPh...16g3038P). doi:10.1088/1367-2630/16/7/073038 (https://doi.org/10.1088%2F1367-2630%2F16%2F7%2F073038). S2CID 118699151 (https://api.semanticscholar.org/CorpusID:118699151).
    - Wei, Yuchuan (2016). "Comment on 'Fractional quantum mechanics' and 'Fractional Schrödinger equation' ". *Physical Review E*. **93** (6). 066103. arXiv:1607.01356 (https://arxiv.org/abs/1607.01356). Bibcode:2016PhRvE..93f6103W (https://ui.adsabs.harvard.edu/abs/2016PhRvE..93f6103W). doi:10.1103/PhysRevE.93.066103 (https://doi.org/10.1103%2FPhysRevE.93.066103). PMID 27415397 (https://pubmed.ncbi.nlm.nih.gov/27415397). S2CID 20010251 (https://api.semanticscholar.org/CorpusID:20010251).
- First experiments with photons:
    - Bouwmeester et al. 1997
    - Boschi et al. 1998
    - Kim, Y.-H.; Kulik, S.P.; Shih, Y. (2001). "Quantum teleportation of a polarization state with a complete bell state measurement". *Phys. Rev. Lett*. **86** (7): 1370–1373. arXiv:quant-ph/0010046 (https://arxiv.org/abs/quant-ph/0010046). Bibcode:2001PhRvL..86.1370K (https://ui.adsabs.harvard.edu/abs/2001PhRvL..86.1370K). doi:10.1103/PhysRevLett.86.1370 (https://doi.org/10.1103%2FPhysRevLett.86.1370). PMID 11178086 (https://pubmed.ncbi.nlm.nih.gov/11178086). S2CID 6123495 (https://api.semanticscholar.org/CorpusID:6123495).
    - Marcikic, I.; Tittel, W.; Zbinden, H.; Gisin, N. (2003). "Long-Distance Teleportation of Qubits at Telecommunication Wavelengths". *Nature*. **421** (6922): 509–513. arXiv:quant-ph/0301178 (https://arxiv.org/abs/quant-ph/0301178). Bibcode:2003Natur.421..509M (https://ui.adsabs.harvard.edu/abs/2003Natur.421..509M). doi:10.1038/nature01376 (https://doi.org/10.1038%2Fnature01376). PMID 12556886 (https://pubmed.ncbi.nlm.nih.gov/12556886). S2CID 4303767 (https://api.semanticscholar.org/CorpusID:4303767).
    - Ursin, Rupert; Jennewein, Thomas; Aspelmeyer, Markus; Kaltenbaek, Rainer; Lindenthal, Michael; Walther, Philip; Zeilinger, Anton (August 2004). "Quantum Teleportation Link across the Danube" (https://doi.org/10.1038%2F430849a). *Nature*. **430** (7002): 849. Bibcode:2004Natur.430..849U (https://ui.adsabs.harvard.edu/abs/2004Natur.430..849U). doi:10.1038/430849a (https://doi.org/10.1038%2F430849a). PMID 15318210 (https://pubmed.ncbi.nlm.nih.gov/15318210). S2CID 4426035 (https://api.semanticscholar.org/CorpusID:4426035).
- First experiments with atoms:
    - Riebe, M.; Häffner, H.; Roos, C. F.; Hänsel, W.; Ruth, M.; Benhelm, J.; Lancaster, G. P. T.; Körber, T. W.; Becher, C.; Schmidt-Kaler, F.; James, D. F. V.; Blatt, R. (2004). "Deterministic Quantum Teleportation with Atoms". *Nature*. **429** (6993): 734–737. Bibcode:2004Natur.429..734R (https://ui.adsabs.harvard.edu/abs/2004Natur.429..734R). doi:10.1038/nature02570 (https://doi.org/10.1038%2Fnature02570). PMID 15201903 (https://pubmed.ncbi.nlm.nih.gov/15201903). S2CID 4397716 (https://api.semanticscholar.org/CorpusID:4397716).
    - Barrett, M. D.; Chiaverini, J.; Schaetz, T.; Britton, J.; Itano, W. M.; Jost, J. D.; Knill, E.; Langer, C.; Leibfried, D.; Ozeri, R.; Wineland, D. J. (2004). "Deterministic Quantum

Teleportation of Atomic Qubits". *Nature*. **429** (6993): 737–739. Bibcode:2004Natur.429..737B (https://ui.adsabs.harvard.edu/abs/2004Natur.429..737B). doi:10.1038/nature02608 (https://doi.org/10.1038%2Fnature02608). PMID 15201904 (https://pubmed.ncbi.nlm.nih.gov/15201904). S2CID 1608775 (https://api.semanticscholar.org/CorpusID:1608775).

- Olmschenk, S.; Matsukevich, D. N.; Maunz, P.; Hayes, D.; Duan, L.-M.; Monroe, C. (2009). "Quantum Teleportation between Distant Matter Qubits". *Science*. **323** (5913): 486–489. arXiv:0907.5240 (https://arxiv.org/abs/0907.5240). Bibcode:2009Sci...323..486O (https://ui.adsabs.harvard.edu/abs/2009Sci...323..486O). doi:10.1126/science.1167209 (https://doi.org/10.1126%2Fscience.1167209). PMID 19164744 (https://pubmed.ncbi.nlm.nih.gov/19164744). S2CID 206516918 (https://api.semanticscholar.org/CorpusID:206516918).

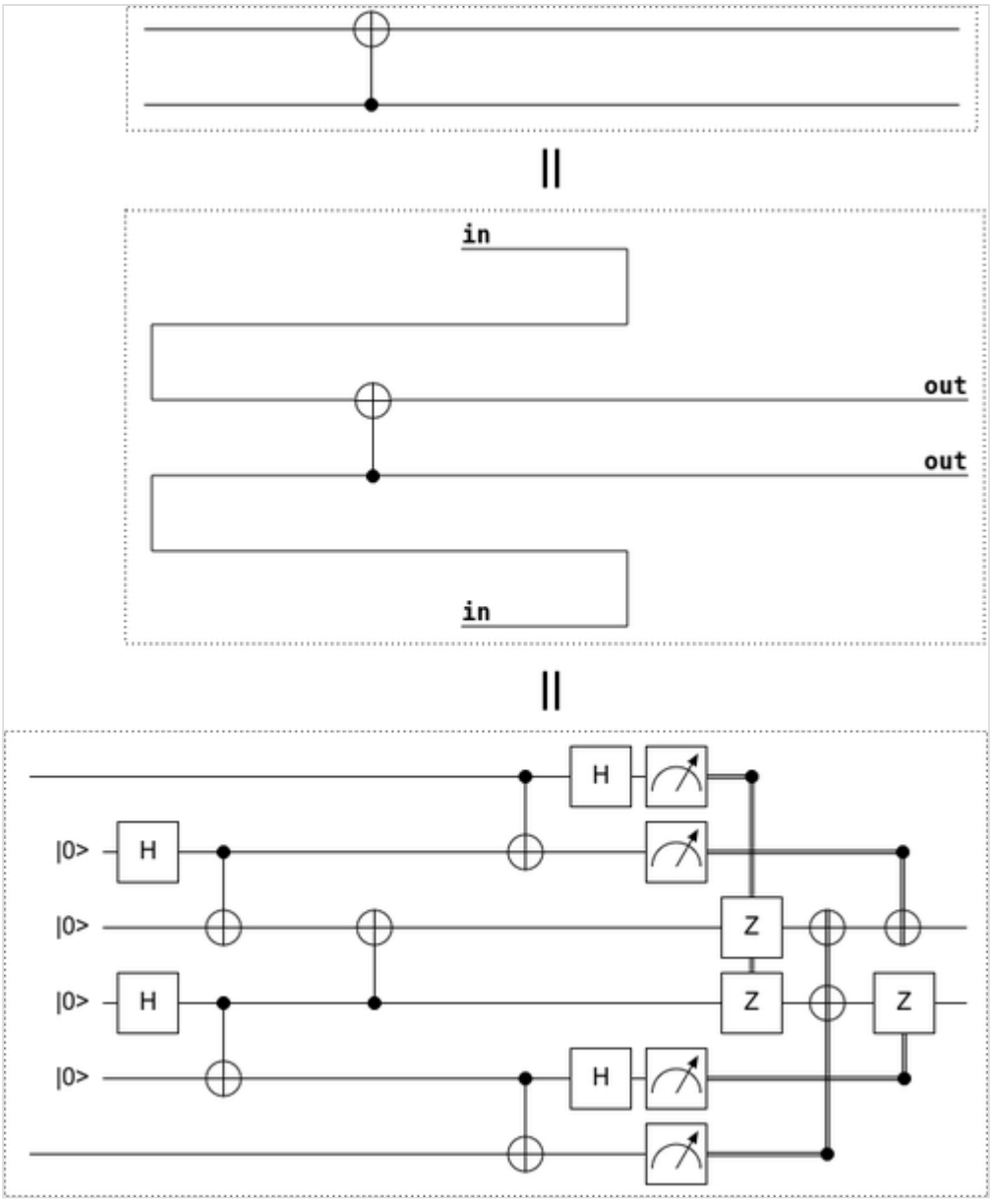
External links

- Loophole-free Bell test (https://web.archive.org/web/20180704082456/http://hansonlab.tudelft.nl/loophole-free-bell-test/) – Kavli Institute of Nanoscience
- "Spooky action and beyond" (http://www.signandsight.com/features/614.html) – Interview with Anton Zeilinger about quantum teleportation. Date: 2006-02-16
- Quantum Teleportation at IBM (http://www.research.ibm.com/quantuminfo/teleportation/) Archived (https://web.archive.org/web/20110107152340/http://www.research.ibm.com/quantuminfo/teleportation/) 7 January 2011 at the Wayback Machine
- Physicists Succeed In Transferring Information Between Matter And Light (http://www.spacedaily.com/news/physics-04zi.html)
- Quantum telecloning: Captain Kirk's clone and the eavesdropper (http://www.physorg.com/news10924.html)
- "Teleportation-based approaches to universal quantum computation" (https://web.archive.org/web/20081218105859/http://www.math.uwaterloo.ca/~amchilds/talks/pi03.ppt). Archived from the original (http://www.math.uwaterloo.ca/~amchilds/talks/pi03.ppt) on 2008-12-18.
- Riebe, M; Chwalla, M; Benhelm, J; Häffner, H; Hänsel, W; Roos, C F; Blatt, R (4 July 2007). "Quantum teleportation with atoms: quantum process tomography". *New Journal of Physics*. **9** (7): 211. arXiv:0704.2027 (https://arxiv.org/abs/0704.2027). Bibcode:2007NJPh....9..211R (https://ui.adsabs.harvard.edu/abs/2007NJPh....9..211R). doi:10.1088/1367-2630/9/7/211 (https://doi.org/10.1088%2F1367-2630%2F9%2F7%2F211).
- Entangled State Teleportation (https://web.archive.org/web/20081218105900/http://www.imit.kth.se/QEO/qucomm/DelD19QuComm.pdf)
- Oh, Sangchul; Lee, Soonchil; Lee, Hai-woong (27 August 2002). "Fidelity of quantum teleportation through noisy channels". *Physical Review A*. **66** (2): 022316. arXiv:quant-ph/0206173 (https://arxiv.org/abs/quant-ph/0206173). Bibcode:2002PhRvA..66b2316O (https://ui.adsabs.harvard.edu/abs/2002PhRvA..66b2316O). doi:10.1103/PhysRevA.66.022316 (https://doi.org/10.1103%2FPhysRevA.66.022316). hdl:10203/1029 (https://hdl.handle.net/10203%2F1029).
- TelePOVM – A generalized quantum teleportation scheme (https://www.cs.technion.ac.il/~talmo/CV/my-new-papers/BHM04-IBM.pdf)
- Entanglement Teleportation via Werner States (https://web.archive.org/web/20081218105859/http://web.am.qub.ac.uk/users/m.s.kim/PRL04236.pdf)
- Quantum Teleportation of a Polarization State (https://web.archive.org/web/20130210090550/http://www.physics.ohio-state.edu/~wilkins/writing/Assign/topics/Q-trans-prl.pdf)
- Childress, David Hatcher (1999). *The Time Travel Handbook: A Manual of Practical Teleportation & Time Travel*. Adventures Unlimited Press. ISBN 978-0-932813-68-8.

- Riebe, M.; Häffner, H.; Roos, C. F.; Hänsel, W.; Benhelm, J.; Lancaster, G. P. T.; Körber, T. W.; Becher, C.; Schmidt-Kaler, F.; James, D. F. V.; Blatt, R. (June 2004). "Deterministic quantum teleportation with atoms". *Nature*. **429** (6993): 734–737. Bibcode:2004Natur.429..734R (https://ui.adsabs.harvard.edu/abs/2004Natur.429..734R). doi:10.1038/nature02570 (https://doi.org/10.1038%2Fnature02570). PMID 15201903 (https://pubmed.ncbi.nlm.nih.gov/15201903).
- Kim, Yoon-Ho; Kulik, Sergei; Shih, Yanhua (January 2002). "Quantum teleportation with a complete Bell state measurement". *Journal of Modern Optics*. **49** (1–2): 221–236. arXiv:quant-ph/0010046 (https://arxiv.org/abs/quant-ph/0010046). Bibcode:2002JMOp...49..221K (https://ui.adsabs.harvard.edu/abs/2002JMOp...49..221K). doi:10.1080/09500340110087633 (https://doi.org/10.1080%2F09500340110087633).
- "Welcome to the quantum Internet" (https://web.archive.org/web/20121130091556/http://www.sciencenews.org/view/feature/id/34762/title/Welcome_to_the_Quantum_Internet). *Science News*. 16 August 2008. Archived from the original (http://sciencenews.org/view/feature/id/34762/title/Welcome_to_the_Quantum_Internet) on 2012-11-30. Retrieved 2008-08-14.
- Quantum experiments – interactive. (http://www.QuantumLab.de)
- A (mostly serious) introduction to quantum teleportation for non-physicists (http://lightlike.com/teleport/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_teleportation&oldid=1245149181"

Quantum gate teleportation



Applying a CNOT gate by using gate teleportation. Uses Bell basis measurement (decomposed here into a CNOT, an H, and two measurements), Bell basis initialization (decomposed here into two resets, an H, and a CNOT), and classical feedback in the form of Pauli operations controlled by the measurement results.

Quantum gate teleportation is a quantum circuit construction where a gate is applied to target qubits by first applying the gate to an entangled state and then teleporting the target qubits through that entangled state. [1][2]

This separation of the physical application of the gate from the target qubit can be useful in cases where applying the gate directly to the target qubit may be more likely to destroy it than to apply the desired operation. For example, the KLM protocol can be used to implement a Controlled NOT gate on a photonic quantum computer, but the process can be prone to errors that destroy the target qubits. By using

gate teleportation, the CNOT operation can be applied to a state that can be easily recreated if it is destroyed, allowing the KLM CNOT to be used in long-running quantum computations without risking the rest of the computation. Additionally, gate teleportation is a key component of magic state distillation, a technique that can be used to overcome the limitations of the Eastin-Knill theorem. [3]

Quantum gate teleportation has been demonstrated in various types of quantum computers, including linear optical, [4] superconducting quantum computing, [5] and trapped ion quantum computing. [6]

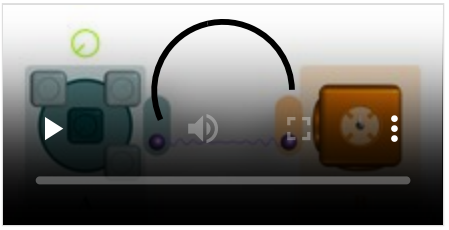
References

1. Jozsa, Richard (2005). "An introduction to measurement based quantum computation". arXiv:quant-ph/0508124 (https://arxiv.org/abs/quant-ph/0508124). Bibcode:2005quant.ph..8124J (https://ui.adsabs.harvard.edu/abs/2005quant.ph..8124J). {{cite journal}}: Cite journal requires |journal= (help)
2. Colin P. Williams (2010). *Explorations in Quantum Computing*. Springer. pp. 633–641. ISBN 978-1-4471-6801-0.
3. Gottesman, Daniel; Chuang, Isaac L. (1999). "Quantum Teleportation is a Universal Computational Primitive". *Nature*. **402** (6760): 390–393. arXiv:quant-ph/9908010 (https://arxiv.org/abs/quant-ph/9908010). Bibcode:1999Natur.402..390G (https://ui.adsabs.harvard.edu/abs/1999Natur.402..390G). doi:10.1038/46503 (https://doi.org/10.1038%2F46503). S2CID 4411647 (https://api.semanticscholar.org/CorpusID:4411647).
4. Chou, K.S.; Blumoff, J.Z.; Wang, C.S.; Reinhold, P.C.; Axline, C.J.; Gao, Y.Y.; Frunzio, L.; Devoret, M.H.; Jiang, Liang; Schoelkopf, R.J. (2010). "Teleportation-based realization of an optical quantum two-qubit entangling gate" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3000260). *PNAS*. **107** (49): 20869–20874. arXiv:1011.0772 (https://arxiv.org/abs/1011.0772). Bibcode:2010PNAS..10720869G (https://ui.adsabs.harvard.edu/abs/2010PNAS..10720869G). doi:10.1073/pnas.1005720107 (https://doi.org/10.1073%2Fpnas.1005720107). PMC 3000260 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3000260). PMID 21098305 (https://pubmed.ncbi.nlm.nih.gov/21098305).
5. Gao, Wei-Bo; Poulin, David (2018). "Deterministic teleportation of a quantum gate between two logical qubits". *Nature*. **561** (7723): 368–373. arXiv:1801.05283 (https://arxiv.org/abs/1801.05283). Bibcode:2018Natur.561..368C (https://ui.adsabs.harvard.edu/abs/2018Natur.561..368C). doi:10.1038/s41586-018-0470-y (https://doi.org/10.1038%2Fs41586-018-0470-y). PMID 30185908 (https://pubmed.ncbi.nlm.nih.gov/30185908). S2CID 3820071 (https://api.semanticscholar.org/CorpusID:3820071).
6. Wan, Yong; Kienzler, Daniel; Erickson, Stephen D.; Mayer, Karl H.; Tan, Ting Rei; Wu, Jenny J.; Vasconcelos, Hilma M.; Glancy, Scott; Knill, Emanuel; Wineland, David J.; Wilson, Andrew C.; Leibfried, Dietrich (2019). "Quantum gate teleportation between separated qubits in a trapped-ion processor". *Science*. **364** (6443): 875–878. arXiv:1902.02891 (https://arxiv.org/abs/1902.02891). Bibcode:2019Sci...364..875W (https://ui.adsabs.harvard.edu/abs/2019Sci...364..875W). doi:10.1126/science.aaw9415 (https://doi.org/10.1126%2Fscience.aaw9415). PMID 31147517 (https://pubmed.ncbi.nlm.nih.gov/31147517). S2CID 119088844 (https://api.semanticscholar.org/CorpusID:119088844).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_gate_teleportation&oldid=1181031724"

WIKIPEDIA
The Free Encyclopedia

Superdense coding



Schematic video demonstrating individual steps of superdense coding. A message consisting of two bits (in video these are (1, 0)) is sent from station A to station B using only a single particle. This particle is a member of an entangled pair created by source S. Station A at first applies a properly chosen operation to its particle and then sends it to station B, which measures both particles in the Bell basis. The measurement result retrieves the two bits sent by station A.

In quantum information theory, **superdense coding** (also referred to as *dense coding*) is a quantum communication protocol to communicate a number of classical bits of information by only transmitting a smaller number of qubits, under the assumption of sender and receiver pre-sharing an entangled resource. In its simplest form, the protocol involves two parties, often referred to as Alice and Bob in this context, which share a pair of maximally entangled qubits, and allows Alice to transmit two bits (i.e., one of 00, 01, 10 or 11) to Bob by sending only one qubit.[1][2] This protocol was first proposed by Charles H. Bennett and Stephen Wiesner in 1970[3] (though not published by them until 1992) and experimentally actualized in 1996 by Klaus Mattle, Harald Weinfurter, Paul G. Kwiat and Anton Zeilinger using entangled photon pairs.[2] Superdense coding can be thought of as the opposite of quantum teleportation, in which one transfers one qubit from Alice to Bob by communicating two classical bits, as long as Alice and Bob have a pre-shared Bell pair.[2]

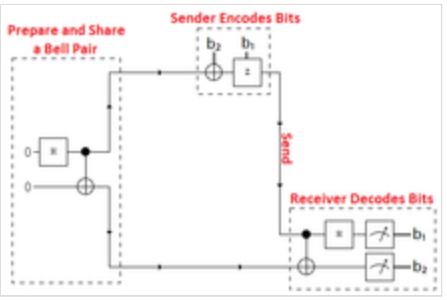
The transmission of two bits via a single qubit is made possible by the fact that Alice can choose among *four* quantum gate operations to perform on her share of the entangled state. Alice determines which operation to perform accordingly to the pair of bits she wants to transmit. She then sends Bob the qubit state *evolved through the chosen gate*. Said qubit thus encodes information about the two bits Alice used to select the operation, and this information can be retrieved by Bob thanks to pre-shared entanglement between them. After receiving Alice's qubit, operating on the pair and measuring both, Bob obtains two classical bits of information. It is worth stressing that if Alice and Bob do not pre-share entanglement, then the superdense protocol is impossible, as this would violate Holevo's theorem.

Superdense coding is the underlying principle of secure quantum secret coding. The necessity of having both qubits to decode the information being sent eliminates the risk of eavesdroppers intercepting messages.[4]

Overview

Suppose Alice wants to send two classical bits of information (00, 01, 10, or 11) to Bob using qubits (instead of classical bits). To do this, an entangled state (e.g. a Bell state) is prepared using a Bell circuit or gate by Charlie, a third person. Charlie then sends one of these qubits (in the Bell state) to Alice and the other to Bob. Once Alice obtains her qubit in the entangled state, she applies a certain quantum gate to her qubit depending on which two-bit message (00, 01, 10 or 11) she wants to send to Bob. Her entangled

qubit is then sent to Bob who, after applying the appropriate quantum gate and making a measurement, can retrieve the classical two-bit message. Observe that Alice does not need to communicate to Bob which gate to apply in order to obtain the correct classical bits from his projective measurement.



When the sender and receiver share a Bell state, two classical bits can be packed into one qubit. In the diagram, lines carry qubits, while the doubled lines carry classic bits. The variables b_1 and b_2 are classic boolean, and the zeroes at the left hand side represent the pure quantum state $|0\rangle$. See the section named "The protocol" below for more details regarding this picture.

The protocol

The protocol can be split into five different steps: preparation, sharing, encoding, sending, and decoding.

Preparation

The protocol starts with the preparation of an entangled state, which is later shared between Alice and Bob. For example, the following Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

is prepared, where $\otimes$ denotes the tensor product. In common usage the tensor product symbol $\otimes$ may be omitted:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle).$$

Sharing

After the preparation of the Bell state $|\Phi^+\rangle$, the qubit denoted by subscript *A* is sent to Alice and the qubit denoted by subscript *B* is sent to Bob. Alice and Bob may be in different locations, an unlimited distance from each other.

There may be an arbitrary period between the preparation and sharing of the entangled state $|\Phi^+\rangle$ and the rest of the steps in the procedure.

Encoding

By applying a quantum gate to her qubit locally, Alice can transform the entangled state $|\Phi^+\rangle$ into any of the four Bell states (including, of course, $|\Phi^+\rangle$). Note that this process cannot "break" the entanglement between the two qubits.

Let's now describe which operations Alice needs to perform on her entangled qubit, depending on which classical two-bit message she wants to send to Bob. We'll later see why these specific operations are performed. There are four cases, which correspond to the four possible two-bit strings that Alice may want to send.

1. If Alice wants to send the classical two-bit string 00 to Bob, then she applies the identity quantum gate, $\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, to her qubit, so that it remains unchanged. The resultant entangled state is then

$$|B_{00}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle)$$

In other words, the entangled state shared between Alice and Bob has not changed, i.e. it is still $|\Phi^+\rangle$. The notation $|B_{00}\rangle$ indicates that Alice wants to send the two-bit string 00.

2. If Alice wants to send the classical two-bit string 01 to Bob, then she applies the quantum *NOT* (or *bit-flip*) gate, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, to her qubit, so that the resultant entangled quantum state becomes

$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|1_A 0_B\rangle + |0_A 1_B\rangle)$$

3. If Alice wants to send the classical two-bit string 10 to Bob, then she applies the quantum *phase-flip* gate $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ to her qubit, so the resultant entangled state becomes

$$|B_{10}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle)$$

4. If, instead, Alice wants to send the classical two-bit string 11 to Bob, then she applies the quantum gate $Z * X = iY = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ to her qubit, so that the resultant entangled state becomes

$$|B_{11}\rangle = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle)$$

The matrices X, Z, and Y are known as Pauli matrices.

Sending

After having performed one of the operations described above, Alice can send her entangled qubit to Bob using a quantum network through some conventional physical medium.

Decoding

In order for Bob to find out which classical bits Alice sent he will perform the CNOT unitary operation, with A as control qubit and B as target qubit. Then, he will perform $H \otimes I$ unitary operation on the entangled qubit A. In other words, the Hadamard quantum gate H is only applied to A (see the figure above).

- If the resultant entangled state was B_{00} then after the application of the above unitary operations the entangled state will become $|00\rangle$

- If the resultant entangled state was B_{01} then after the application of the above unitary operations the entangled state will become $|01\rangle$
- If the resultant entangled state was B_{10} then after the application of the above unitary operations the entangled state will become $|10\rangle$
- If the resultant entangled state was B_{11} then after the application of the above unitary operations the entangled state will become $|11\rangle$

These operations performed by Bob can be seen as a measurement which projects the entangled state onto one of the four two-qubit basis vectors $|00\rangle, |01\rangle, |10\rangle$ or $|11\rangle$ (as you can see from the outcomes and the example below).

Example

For example, if the resultant entangled state (after the operations performed by Alice) was $B_{01} = \frac{1}{\sqrt{2}}(|1_A 0_B\rangle + |0_A 1_B\rangle)$, then a CNOT with A as control bit and B as target bit will change B_{01} to become $B'_{01} = \frac{1}{\sqrt{2}}(|1_A 1_B\rangle + |0_A 1_B\rangle)$. Now, the Hadamard gate is applied only to A, to obtain

$$B''_{01} = \frac{1}{\sqrt{2}}\left[\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)_A \otimes |1_B\rangle + \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)_A \otimes |1_B\rangle\right].$$

For simplicity, subscripts may be removed:

$$\begin{aligned} B''_{01} &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle + \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) + \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)\right) = \tfrac{1}{2}|01\rangle - \tfrac{1}{2}|11\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|11\rangle = |01\rangle. \end{aligned}$$

Now, Bob has the basis state **Failed to parse (SVG (MathML can be enabled via browser plugin): Invalid response ("Math extension cannot connect to Restbase.") from server "http://localhost:6011/en.wikipedia.org/v1/":): {\displaystyle |01\rangle}** , so he knows that Alice wanted to send the two-bit string 01.

Security

Superdense coding is a form of secure quantum communication.[4] If an eavesdropper, commonly called Eve, intercepts Alice's qubit en route to Bob, all that is obtained by Eve is part of an entangled state. Without access to Bob's qubit, Eve is unable to get any information from Alice's qubit. A third party is unable to eavesdrop on information being communicated through superdense coding and an attempt to measure either qubit would collapse the state of that qubit and alert Bob and Alice.

General dense coding scheme

General dense coding schemes can be formulated in the language used to describe quantum channels. Alice and Bob share a maximally entangled state ω. Let the subsystems initially possessed by Alice and Bob be labeled 1 and 2, respectively. To transmit the message x, Alice applies an appropriate channel

$$\Phi_x$$

on subsystem 1. On the combined system, this is effected by

$$\omega \to (\Phi_x \otimes I)(\omega)$$

where I denotes the identity map on subsystem 2. Alice then sends her subsystem to Bob, who performs a measurement on the combined system to recover the message. Let Bob's measurement be modelled by a POVM $\{F_y\}_y$, with F_y positive semidefinite operators such that $\sum_y F_y = I$. The probability that Bob's measuring apparatus registers the message y is thus

$$p(y|x) = \langle F_y, (\Phi_x \otimes I)(\omega) \rangle \equiv \mathrm{Tr}[F_y(\Phi_x \otimes I)(\omega)].$$

Therefore, to achieve the desired transmission, we require that

$$p(y|x) = \mathrm{Tr}[F_y(\Phi_x \otimes I)(\omega)] = \delta_{xy},$$

where δ_{xy} is the Kronecker delta.

Experimental

The protocol of superdense coding has been actualized in several experiments using different systems to varying levels of channel capacity and fidelities. In 2004, trapped beryllium-9 ions were used in a maximally entangled state to achieve a channel capacity of 1.16 with a fidelity of 0.85.[5] In 2017, a channel capacity of 1.665 was achieved with a fidelity of 0.87 through optical fibers.[6] High-dimensional ququarts (states formed in photon pairs by non-degenerate spontaneous parametric down-conversion) were used to reach a channel capacity of 2.09 (with a limit of 2.32) with a fidelity of 0.98.[7] Nuclear magnetic resonance (NMR) has also been used to share among three parties.[8]

References

1. Bennett, C.; Wiesner, S. (1992). "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". *Physical Review Letters*. **69** (20): 2881–2884. Bibcode:1992PhRvL..69.2881B (https://ui.adsabs.harvard.edu/abs/1992PhRvL..69.2881B). doi:10.1103/PhysRevLett.69.2881 (https://doi.org/10.1103%2FPhysRevLett.69.2881). PMID 10046665 (https://pubmed.ncbi.nlm.nih.gov/10046665).
2. Nielsen, Michael A.; Chuang, Isaac L. (9 December 2010). "2.3 Application: superdense coding". *Quantum Computation and Quantum Information: 10th Anniversary Edition* (https://books.google.com/books?id=-s4DEy7o-a0C). Cambridge University Press. p. 97. ISBN 978-1-139-49548-6.
3. Stephen Wiesner (https://orsattath.wordpress.com/2021/08/14/stephen-wiesner/). Memorial blog post by Or Sattath, with scan of Bennett's handwritten notes from 1970. See also Stephen Wiesner (1942–2021) (https://www.scottaaronson.com/blog/?p=5730) by Scott Aaronson, which also discusses this topic.
4. Wang, C., Deng, F.-G., Li, Y.-S., Liu, X.-S., & Long, G. L. (2005). Quantum secure direct communication with high-dimension quantum superdense coding. Physical Review A, 71(4).
5. Schaetz, T., Barrett, M. D., Leibfried, D., Chiaverini, J., Britton, J., Itano, W. M., … Wineland, D. J. (2004). Quantum Dense Coding with Atomic Qubits. Physical Review Letters, 93(4).
6. Williams, B. P., Sadlier, R. J., & Humble, T. S. (2017). Superdense Coding over Optical Fiber Links with Complete Bell-State Measurements. Physical Review Letters, 118(5).

7. Hu, X.-M., Guo, Y., Liu, B.-H., Huang, Y.-F., Li, C.-F., & Guo, G.-C. (2018). Beating the channel capacity limit for superdense coding with entangled ququarts. Science Advances, 4(7), eaat9304.
8. Wei, D., Yang, X., Luo, J., Sun, X., Zeng, X., & Liu, M. (2004). NMR experimental implementation of three-parties quantum superdense coding. Chinese Science Bulletin, 49(5), 423–426.

- Wilde, Mark M., 2017, Quantum Information Theory, Cambridge University Press (http://www.cambridge.org/us/academic/subjects/computer-science/cryptography-cryptology-and-coding/quantum-information-theory-2nd-edition), Also available at eprint arXiv:1106.1145 (https://arxiv.org/abs/1106.1445)

External links

- Qubits, Quantum Mechanics and Computers Course Notes (http://www-inst.eecs.berkeley.edu/~cs191/fa09/lectures/lecture6_fa09.pdf)
- Superdense coding: how to send two bits using one qubit (https://www.youtube.com/watch?v=w5rCn593Dig) on YouTube by Michael Nielsen

Retrieved from "https://en.wikipedia.org/w/index.php?title=Superdense_coding&oldid=1234973238"

WIKIPEDIA
The Free Encyclopedia

Quantum cryptography

Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks.[1][2] The best known example of quantum cryptography is quantum key distribution, which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed due to wave function collapse (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution (QKD).

History

In the early 1970s, Stephen Wiesner, then at Columbia University in New York, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by the IEEE Information Theory Society but was eventually published in 1983 in *SIGACT News*.[3] In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of photons,[4] so that either, but not both, properties may be received and decoded. It was not until Charles H. Bennett, of the IBM's Thomas J. Watson Research Center, and Gilles Brassard met in 1979 at the 20th IEEE Symposium on the Foundations of Computer Science, held in Puerto Rico, that they discovered how to incorporate Wiesner's findings. "The main breakthrough came when we realized that photons were never meant to store information, but rather to transmit it."[3] In 1984, building upon this work, Bennett and Brassard proposed a method for secure communication, which is now called BB84.[5] Independently, in 1991 Artur Ekert proposed to use Bell's inequalities to achieve secure key distribution.[6] Ekert's protocol for the key distribution, as it was subsequently shown by Dominic Mayers and Andrew Yao, offers device-independent quantum key distribution.

Companies that manufacture quantum cryptography systems include MagiQ Technologies, Inc. (Boston), ID Quantique (Geneva), QuintessenceLabs (Canberra, Australia), Toshiba (Tokyo), QNu Labs (India) and SeQureNet (Paris).

Advantages

Cryptography is the strongest link in the chain of data security.[7] However, interested parties cannot assume that cryptographic keys will remain secure indefinitely.[8] Quantum cryptography[2] has the potential to encrypt data for longer periods than classical cryptography.[8] Using classical cryptography, scientists cannot guarantee encryption beyond approximately 30 years, but some stakeholders could use longer periods of protection.[8] Take, for example, the healthcare industry. As of 2017, 85.9% of office-based physicians are using electronic medical record systems to store and transmit patient data.[9] Under the Health Insurance Portability and Accountability Act, medical records must be kept secret.[10] Quantum key distribution can protect electronic records for periods of up to 100 years.[8] Also, quantum

cryptography has useful applications for governments and militaries as, historically, governments have kept military data secret for periods of over 60 years.[8] There also has been proof that quantum key distribution can travel through a noisy channel over a long distance and be secure. It can be reduced from a noisy quantum scheme to a classical noiseless scheme. This can be solved with classical probability theory.[11] This process of having consistent protection over a noisy channel can be possible through the implementation of quantum repeaters. Quantum repeaters have the ability to resolve quantum communication errors in an efficient way. Quantum repeaters, which are quantum computers, can be stationed as segments over the noisy channel to ensure the security of communication. Quantum repeaters do this by purifying the segments of the channel before connecting them creating a secure line of communication. Sub-par quantum repeaters can provide an efficient amount of security through the noisy channel over a long distance.[11]

Applications

Quantum cryptography is a general subject that covers a broad range of cryptographic practices and protocols. Some of the most notable applications and protocols are discussed below.

Quantum key distribution

The best-known and developed application of quantum cryptography is QKD, which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, discrepancies will arise causing Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used for symmetric cryptography (e.g. one-time pad).

The security of quantum key distribution can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution. This is usually described as "unconditional security", although there are some minimal assumptions required, including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack would be possible.

While QKD is secure, its practical application faces some challenges. There are in fact limitations for the key generation rate at increasing transmission distances.[12][13][14] Recent studies have allowed important advancements in this regard. In 2018, the protocol of twin-field QKD[15] was proposed as a mechanism to overcome the limits of lossy communication. The rate of the twin field protocol was shown to overcome the secret key-agreement capacity of the lossy communication channel, known as repeater-less PLOB bound,[14] at 340 km of optical fiber; its ideal rate surpasses this bound already at 200 km and follows the rate-loss scaling of the higher repeater-assisted secret key-agreement capacity[16] (see figure 1 of[15] and figure 11 of[2] for more details). The protocol suggests that optimal key rates are achievable on "550 kilometers of standard optical fibre", which is already commonly used in communications today. The theoretical result was confirmed in the first experimental demonstration of QKD beyond the PLOB bound

which has been characterized as the first *effective* quantum repeater.[17] Notable developments in terms of achieving high rates at long distances are the sending-not-sending (SNS) version of the TF-QKD protocol.[18][19] and the no-phase-postselected twin-field scheme.[20]

Mistrustful quantum cryptography

In mistrustful cryptography the participating parties do not trust each other. For example, Alice and Bob collaborate to perform some computation where both parties enter some private inputs. But Alice does not trust Bob and Bob does not trust Alice. Thus, a secure implementation of a cryptographic task requires that after completing the computation, Alice can be guaranteed that Bob has not cheated and Bob can be guaranteed that Alice has not cheated either. Examples of tasks in mistrustful cryptography are commitment schemes and secure computations, the latter including the further examples of coin flipping and oblivious transfer. Key distribution does not belong to the area of mistrustful cryptography. Mistrustful quantum cryptography studies the area of mistrustful cryptography using quantum systems.

In contrast to quantum key distribution where unconditional security can be achieved based only on the laws of quantum physics, in the case of various tasks in mistrustful cryptography there are no-go theorems showing that it is impossible to achieve unconditionally secure protocols based only on the laws of quantum physics. However, some of these tasks can be implemented with unconditional security if the protocols not only exploit quantum mechanics but also special relativity. For example, unconditionally secure quantum bit commitment was shown impossible by Mayers[21] and by Lo and Chau.[22] Unconditionally secure ideal quantum coin flipping was shown impossible by Lo and Chau.[23] Moreover, Lo showed that there cannot be unconditionally secure quantum protocols for one-out-of-two oblivious transfer and other secure two-party computations.[24] However, unconditionally secure relativistic protocols for coin flipping and bit-commitment have been shown by Kent.[25][26]

Quantum coin flipping

Unlike quantum key distribution, quantum coin flipping is a protocol that is used between two participants who do not trust each other.[27] The participants communicate via a quantum channel and exchange information through the transmission of qubits.[28] But because Alice and Bob do not trust each other, each expects the other to cheat. Therefore, more effort must be spent on ensuring that neither Alice nor Bob can gain a significant advantage over the other to produce a desired outcome. An ability to influence a particular outcome is referred to as a bias, and there is a significant focus on developing protocols to reduce the bias of a dishonest player,[29][30] otherwise known as cheating. Quantum communication protocols, including quantum coin flipping, have been shown to provide significant security advantages over classical communication, though they may be considered difficult to realize in the practical world.[31]

A coin flip protocol generally occurs like this:[32]

1. Alice chooses a basis (either rectilinear or diagonal) and generates a string of photons to send to Bob in that basis.
2. Bob randomly chooses to measure each photon in a rectilinear or diagonal basis, noting which basis he used and the measured value.
3. Bob publicly guesses which basis Alice used to send her qubits.
4. Alice announces the basis she used and sends her original string to Bob.

5. Bob confirms by comparing Alice's string to his table. It should be perfectly correlated with the values Bob measured using Alice's basis and completely uncorrelated with the opposite.

Cheating occurs when one player attempts to influence, or increase the probability of a particular outcome. The protocol discourages some forms of cheating; for example, Alice could cheat at step 4 by claiming that Bob incorrectly guessed her initial basis when he guessed correctly, but Alice would then need to generate a new string of qubits that perfectly correlates with what Bob measured in the opposite table.[32] Her chance of generating a matching string of qubits will decrease exponentially with the number of qubits sent, and if Bob notes a mismatch, he will know she was lying. Alice could also generate a string of photons using a mixture of states, but Bob would easily see that her string will correlate partially (but not fully) with both sides of the table, and know she cheated in the process.[32] There is also an inherent flaw that comes with current quantum devices. Errors and lost qubits will affect Bob's measurements, resulting in holes in Bob's measurement table. Significant losses in measurement will affect Bob's ability to verify Alice's qubit sequence in step 5.

One theoretically surefire way for Alice to cheat is to utilize the Einstein-Podolsky-Rosen (EPR) paradox. Two photons in an EPR pair are anticorrelated; that is, they will always be found to have opposite polarizations, provided that they are measured in the same basis. Alice could generate a string of EPR pairs, sending one photon per pair to Bob and storing the other herself. When Bob states his guess, she could measure her EPR pair photons in the opposite basis and obtain a perfect correlation to Bob's opposite table.[32] Bob would never know she cheated. However, this requires capabilities that quantum technology currently does not possess, making it impossible to do in practice. To successfully execute this, Alice would need to be able to store all the photons for a significant amount of time as well as measure them with near perfect efficiency. This is because any photon lost in storage or in measurement would result in a hole in her string that she would have to fill by guessing. The more guesses she has to make, the more she risks detection by Bob for cheating.

Quantum commitment

In addition to quantum coin-flipping, quantum commitment protocols are implemented when distrustful parties are involved. A commitment scheme allows a party Alice to fix a certain value (to "commit") in such a way that Alice cannot change that value while at the same time ensuring that the recipient Bob cannot learn anything about that value until Alice reveals it. Such commitment schemes are commonly used in cryptographic protocols (e.g. Quantum coin flipping, Zero-knowledge proof, secure two-party computation, and Oblivious transfer).

In the quantum setting, they would be particularly useful: Crépeau and Kilian showed that from a commitment and a quantum channel, one can construct an unconditionally secure protocol for performing so-called oblivious transfer.[33] Oblivious transfer, on the other hand, had been shown by Kilian to allow implementation of almost any distributed computation in a secure way (so-called secure multi-party computation).[34] (Note: The results by Crépeau and Kilian[33][34] together do not directly imply that given a commitment and a quantum channel one can perform secure multi-party computation. This is because the results do not guarantee "composability", that is, when plugging them together, one might lose security.)

Early quantum commitment protocols[35] were shown to be flawed. In fact, Mayers showed that (unconditionally secure) quantum commitment is impossible: a computationally unlimited attacker can break any quantum commitment protocol.[21]

Yet, the result by Mayers does not preclude the possibility of constructing quantum commitment protocols (and thus secure multi-party computation protocols) under assumptions that are much weaker than the assumptions needed for commitment protocols that do not use quantum communication. The bounded quantum storage model described below is an example for a setting in which quantum communication can be used to construct commitment protocols. A breakthrough in November 2013 offers "unconditional" security of information by harnessing quantum theory and relativity, which has been successfully demonstrated on a global scale for the first time.[36] More recently, Wang et al., proposed another commitment scheme in which the "unconditional hiding" is perfect.[37]

Physical unclonable functions can be also exploited for the construction of cryptographic commitments.[38]

Bounded- and noisy-quantum-storage model

One possibility to construct unconditionally secure quantum commitment and quantum oblivious transfer (OT) protocols is to use the bounded quantum storage model (BQSM). In this model, it is assumed that the amount of quantum data that an adversary can store is limited by some known constant Q. However, no limit is imposed on the amount of classical (i.e., non-quantum) data the adversary may store.

In the BQSM, one can construct commitment and oblivious transfer protocols.[39] The underlying idea is the following: The protocol parties exchange more than Q quantum bits (qubits). Since even a dishonest party cannot store all that information (the quantum memory of the adversary is limited to Q qubits), a large part of the data will have to be either measured or discarded. Forcing dishonest parties to measure a large part of the data allows the protocol to circumvent the impossibility result, commitment and oblivious transfer protocols can now be implemented.[21]

The protocols in the BQSM presented by Damgård, Fehr, Salvail, and Schaffner[39] do not assume that honest protocol participants store any quantum information; the technical requirements are similar to those in quantum key distribution protocols. These protocols can thus, at least in principle, be realized with today's technology. The communication complexity is only a constant factor larger than the bound Q on the adversary's quantum memory.

The advantage of the BQSM is that the assumption that the adversary's quantum memory is limited is quite realistic. With today's technology, storing even a single qubit reliably over a sufficiently long time is difficult. (What "sufficiently long" means depends on the protocol details. By introducing an artificial pause in the protocol, the amount of time over which the adversary needs to store quantum data can be made arbitrarily large.)

An extension of the BQSM is the noisy-storage model introduced by Wehner, Schaffner and Terhal.[40] Instead of considering an upper bound on the physical size of the adversary's quantum memory, an adversary is allowed to use imperfect quantum storage devices of arbitrary size. The level of imperfection is modelled by noisy quantum channels. For high enough noise levels, the same primitives as in the BQSM can be achieved[41] and the BQSM forms a special case of the noisy-storage model.

In the classical setting, similar results can be achieved when assuming a bound on the amount of classical (non-quantum) data that the adversary can store.[42] It was proven, however, that in this model also the honest parties have to use a large amount of memory (namely the square-root of the adversary's memory

bound).[43] This makes these protocols impractical for realistic memory bounds. (Note that with today's technology such as hard disks, an adversary can cheaply store large amounts of classical data.)

Position-based quantum cryptography

The goal of position-based quantum cryptography is to use the *geographical location* of a player as its (only) credential. For example, one wants to send a message to a player at a specified position with the guarantee that it can only be read if the receiving party is located at that particular position. In the basic task of *position-verification*, a player, Alice, wants to convince the (honest) verifiers that she is located at a particular point. It has been shown by Chandran *et al.* that position-verification using classical protocols is impossible against colluding adversaries (who control all positions except the prover's claimed position).[44] Under various restrictions on the adversaries, schemes are possible.

Under the name of 'quantum tagging', the first position-based quantum schemes have been investigated in 2002 by Kent. A US-patent[45] was granted in 2006. The notion of using quantum effects for location verification first appeared in the scientific literature in 2010.[46][47] After several other quantum protocols for position verification have been suggested in 2010,[48][49] Buhrman et al. claimed a general impossibility result:[50] using an enormous amount of quantum entanglement (they use a doubly exponential number of EPR pairs, in the number of qubits the honest player operates on), colluding adversaries are always able to make it look to the verifiers as if they were at the claimed position. However, this result does not exclude the possibility of practical schemes in the bounded- or noisy-quantum-storage model (see above). Later Beigi and König improved the amount of EPR pairs needed in the general attack against position-verification protocols to exponential. They also showed that a particular protocol remains secure against adversaries who controls only a linear amount of EPR pairs.[51] It is argued in[52] that due to time-energy coupling the possibility of formal unconditional location verification via quantum effects remains an open problem. The study of position-based quantum cryptography also has connections with the protocol of port-based quantum teleportation, which is a more advanced version of quantum teleportation, where many EPR pairs are simultaneously used as ports.

Device-independent quantum cryptography

A quantum cryptographic protocol is **device-independent** if its security does not rely on trusting that the quantum devices used are truthful. Thus the security analysis of such a protocol needs to consider scenarios of imperfect or even malicious devices.[53] Mayers and Yao[54] proposed the idea of designing quantum protocols using "self-testing" quantum apparatus, the internal operations of which can be uniquely determined by their input-output statistics. Subsequently, Roger Colbeck in his Thesis[55] proposed the use of Bell tests for checking the honesty of the devices. Since then, several problems have been shown to admit unconditional secure and device-independent protocols, even when the actual devices performing the Bell test are substantially "noisy", i.e., far from being ideal. These problems include quantum key distribution,[56][57] randomness expansion,[57][58] and randomness amplification.[59]

In 2018, theoretical studies performed by Arnon- Friedman et al. suggest that exploiting a property of entropy that is later referred to as "Entropy Accumulation Theorem (EAT)", an extension of Asymptotic equipartition property, can guarantee the security of a device independent protocol.[60]

Post-quantum cryptography

Quantum computers may become a technological reality; it is therefore important to study cryptographic schemes used against adversaries with access to a quantum computer. The study of such schemes is often referred to as post-quantum cryptography. The need for post-quantum cryptography arises from the fact that many popular encryption and signature schemes (schemes based on ECC and RSA) can be broken using Shor's algorithm for factoring and computing discrete logarithms on a quantum computer. Examples for schemes that are, as of today's knowledge, secure against quantum adversaries are McEliece and lattice-based schemes, as well as most symmetric-key algorithms.[61][62] Surveys of post-quantum cryptography are available.[63][64]

There is also research into how existing cryptographic techniques have to be modified to be able to cope with quantum adversaries. For example, when trying to develop zero-knowledge proof systems that are secure against quantum adversaries, new techniques need to be used: In a classical setting, the analysis of a zero-knowledge proof system usually involves "rewinding", a technique that makes it necessary to copy the internal state of the adversary. In a quantum setting, copying a state is not always possible (no-cloning theorem); a variant of the rewinding technique has to be used.[65]

Post quantum algorithms are also called "quantum resistant", because – unlike quantum key distribution – it is not known or provable that there will not be potential future quantum attacks against them. Even though they may possibly be vulnerable to quantum attacks in the future, the NSA is announcing plans to transition to quantum resistant algorithms.[66] The National Institute of Standards and Technology (NIST) believes that it is time to think of quantum-safe primitives.[67]

Quantum cryptography beyond key distribution

So far, quantum cryptography has been mainly identified with the development of quantum key distribution protocols. Symmetric cryptosystems with keys that have been distributed by means of quantum key distribution become inefficient for large networks (many users), because of the necessity for the establishment and the manipulation of many pairwise secret keys (the so-called "key-management problem"). Moreover, this distribution alone does not address many other cryptographic tasks and functions, which are of vital importance in everyday life. Kak's three-stage protocol has been proposed as a method for secure communication that is entirely quantum unlike quantum key distribution, in which the cryptographic transformation uses classical algorithms[68]

Besides quantum commitment and oblivious transfer (discussed above), research on quantum cryptography beyond key distribution revolves around quantum message authentication,[69] quantum digital signatures,[70][71] quantum one-way functions and public-key encryption,[72][73][74][75][76][77][78] quantum fingerprinting[79] and entity authentication[80][81][82] (for example, see Quantum readout of PUFs), etc.

Y-00 protocol

H. P. Yuen presented Y-00 as a stream cipher using quantum noise around 2000 and applied it for the U.S. Defense Advanced Research Projects Agency (DARPA) High-Speed and High-Capacity Quantum Cryptography Project as an alternative to quantum key distribution.[83][84] The review paper summarizes it well.[85]

Unlike quantum key distribution protocols, the main purpose of Y-00 is to transmit a message without eavesdrop-monitoring, not to distribute a key. Therefore, privacy amplification may be used only for key distributions.[86] Currently, research is being conducted mainly in Japan and China: e.g.[87][88]

The principle of operation is as follows. First, legitimate users share a key and change it to a pseudo-random keystream using the same pseudo-random number generator. Then, the legitimate parties can perform conventional optical communications based on the shared key by transforming it appropriately. For attackers who do not share the key, the wire-tap channel model of Aaron D. Wyner is implemented. The legitimate users' advantage based on the shared key is called "advantage creation". The goal is to achieve longer covert communication than the information-theoretic security limit (one-time pad) set by Shannon.[89] The source of the noise in the above wire-tap channel is the uncertainty principle of the electromagnetic field itself, which is a theoretical consequence of the theory of laser described by Roy J. Glauber and E. C. George Sudarshan (coherent state).[90][91][92] Therefore, existing optical communication technologies are sufficient for implementation that some reviews describes: e.g.[85] Furthermore, since it uses ordinary communication laser light, it is compatible with existing communication infrastructure and can be used for high-speed and long-distance communication and routing.[93] [94] [95] [96] [97]

Although the main purpose of the protocol is to transmit the message, key distribution is possible by simply replacing the message with a key.[98][86] Since it is a symmetric key cipher, it must share the initial key previously; however, a method of the initial key agreement was also proposed.[99]

On the other hand, it is currently unclear what implementation realizes information-theoretic security, and security of this protocol has long been a matter of debate.[100][101][102][103][104][105][106][107][108][109]

Implementation in practice

In theory, quantum cryptography seems to be a successful turning point in the information security sector. However, no cryptographic method can ever be absolutely secure.[110] In practice, quantum cryptography is only conditionally secure, dependent on a key set of assumptions.[111]

Single-photon source assumption

The theoretical basis for quantum key distribution assumes the use of single-photon sources. However, such sources are difficult to construct, and most real-world quantum cryptography systems use faint laser sources as a medium for information transfer.[111] These multi-photon sources open the possibility for eavesdropper attacks, particularly a photon splitting attack.[112] An eavesdropper, Eve, can split the multi-photon source and retain one copy for herself.[112] The other photons are then transmitted to Bob without any measurement or trace that Eve captured a copy of the data.[112] Scientists believe they can retain security with a multi-photon source by using decoy states that test for the presence of an eavesdropper.[112] However, in 2016, scientists developed a near perfect single photon source and estimate that one could be developed in the near future.[113]

Identical detector efficiency assumption

In practice, multiple single-photon detectors are used in quantum key distribution devices, one for Alice and one for Bob.[111] These photodetectors are tuned to detect an incoming photon during a short window of only a few nanoseconds.[114] Due to manufacturing differences between the two detectors, their respective detection windows will be shifted by some finite amount.[114] An eavesdropper, Eve, can take advantage of this detector inefficiency by measuring Alice's qubit and sending a "fake state" to Bob.[114] Eve first captures the photon sent by Alice and then generates another photon to send to Bob.[114] Eve manipulates the phase and timing of the "faked" photon in a way that prevents Bob from detecting the presence of an eavesdropper.[114] The only way to eliminate this vulnerability is to eliminate differences in photodetector efficiency, which is difficult to do given finite manufacturing tolerances that cause optical path length differences, wire length differences, and other defects.[114]

Deprecation of quantum key distributions from governmental institutions

Because of the practical problems with quantum key distribution, some governmental organizations recommend the use of post-quantum cryptography (quantum resistant cryptography) instead. For example, the US National Security Agency,[115] European Union Agency for Cybersecurity of EU (ENISA),[116] UK's National Cyber Security Centre,[117] French Secretariat for Defense and Security (ANSSI),[118] and German Federal Office for Information Security (BSI)[119] recommend post-quantum cryptography.

For example, the US National Security Agency addresses five issues:[115]

1. Quantum key distribution is only a partial solution. QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or pre-placed keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.
2. Quantum key distribution requires special purpose equipment. QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.

3. Quantum key distribution increases infrastructure costs and insider-threat risks. QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.
4. Securing and validating quantum key distribution is a significant challenge. The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than what is available in most physical engineering scenarios, making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.[120]
5. Quantum key distribution increases the risk of denial of service. The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

In response to problem 1 above, attempts to deliver authentication keys using post-quantum cryptography (or quantum-resistant cryptography) have been proposed worldwide. On the other hand, quantum-resistant cryptography is cryptography belonging to the class of computational security. In 2015, a research result was already published that "sufficient care must be taken in implementation to achieve information-theoretic security for the system as a whole when authentication keys that are not information-theoretic secure are used" (if the authentication key is not information-theoretically secure, an attacker can break it to bring all classical and quantum communications under control and relay them to launch a man-in-the-middle attack).[121] Ericsson, a private company, also cites and points out the above problems and then presents a report that it may not be able to support the zero trust security model, which is a recent trend in network security technology.[122]

Quantum Cryptography in Education

Quantum cryptography, specifically the BB84 protocol, has become an important topic in physics and computer science education. The challenge of teaching quantum cryptography lies in the technical requirements and the conceptual complexity of quantum mechanics. However, simplified experimental setups for educational purposes are becoming more common [123] , allowing undergraduate students to engage with the core principles of quantum key distribution (QKD) without requiring advanced quantum technology.

References

1. Gisin, Nicolas; Ribordy, Grégoire; Tittel, Wolfgang; Zbinden, Hugo (2002). "Quantum cryptography" (https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.74.145). *Reviews of Modern Physics*. **74** (1): 145–195. arXiv:quant-ph/0101098 (https://arxiv.org/abs/quant-ph/0101098). Bibcode:2002RvMP...74..145G (https://ui.adsabs.harvard.edu/abs/2002RvMP...74..145G). doi:10.1103/RevModPhys.74.145 (https://doi.org/10.1103%2FRevModPhys.74.145). S2CID 6979295 (https://api.semanticscholar.org/CorpusID:6979295).

2. Pirandola, S.; Andersen, U. L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; Pereira, J. L.; et al. (2020). "Advances in quantum cryptography" (https://www.osapublishing.org/aop/abstract.cfm?uri=aop-12-4-1012). *Advances in Optics and Photonics*. **12** (4): 1012–1236. arXiv:1906.01645 (https://arxiv.org/abs/1906.01645). Bibcode:2020AdOP...12.1012P (https://ui.adsabs.harvard.edu/abs/2020AdOP...12.1012P). doi:10.1364/AOP.361502 (https://doi.org/10.1364%2FAOP.361502). S2CID 174799187 (https://api.semanticscholar.org/CorpusID:174799187).
3. Bennett, Charles H.; et al. (1992). "Experimental quantum cryptography" (https://doi.org/10.1007%2Fbf00191318). *Journal of Cryptology*. **5** (1): 3–28. doi:10.1007/bf00191318 (https://doi.org/10.1007%2Fbf00191318). S2CID 206771454 (https://api.semanticscholar.org/CorpusID:206771454).
4. Wiesner, Stephen (1983). "Conjugate coding". *ACM SIGACT News*. **15** (1): 78–88. doi:10.1145/1008908.1008920 (https://doi.org/10.1145%2F1008908.1008920). S2CID 207155055 (https://api.semanticscholar.org/CorpusID:207155055).
5. Bennett, Charles H.; Brassard, Gilles (1984). "Quantum cryptography: Public key distribution and coin tossing". *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. **175**: 8.
6. Ekert, A (1991). "Quantum cryptography based on Bell's theorem". *Physical Review Letters*. **67** (6): 661–663. Bibcode:1991PhRvL..67..661E (https://ui.adsabs.harvard.edu/abs/1991PhRvL..67..661E). doi:10.1103/physrevlett.67.661 (https://doi.org/10.1103%2Fphysrevlett.67.661). PMID 10044956 (https://pubmed.ncbi.nlm.nih.gov/10044956). S2CID 27683254 (https://api.semanticscholar.org/CorpusID:27683254).
7. "Crypto-gram: December 15, 2003 – Schneier on Security" (https://www.schneier.com/crypto-gram/archives/2003/1215.html). *www.schneier.com*. Retrieved 13 October 2020.
8. Stebila, Douglas; Mosca, Michele; Lütkenhaus, Norbert (2010), Sergienko, Alexander; Pascazio, Saverio; Villoresi, Paolo (eds.), "The Case for Quantum Key Distribution" (http://link.springer.com/10.1007/978-3-642-11731-2_35), *Quantum Communication and Quantum Networking*, vol. 36, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 283–296, arXiv:0902.2839 (https://arxiv.org/abs/0902.2839), Bibcode:2010qcqn.book..283S (https://ui.adsabs.harvard.edu/abs/2010qcqn.book..283S), doi:10.1007/978-3-642-11731-2_35 (https://doi.org/10.1007%2F978-3-642-11731-2_35), ISBN 978-3-642-11730-5, S2CID 457259 (https://api.semanticscholar.org/CorpusID:457259), retrieved 13 October 2020
9. "FastStats" (https://www.cdc.gov/nchs/fastats/electronic-medical-records.htm). *www.cdc.gov*. 4 August 2020. Retrieved 13 October 2020.
10. Rights (OCR), Office for Civil (7 May 2008). "Privacy" (https://www.hhs.gov/hipaa/for-professionals/privacy/index.html). *HHS.gov*. Retrieved 13 October 2020.
11. Lo, Hoi-Kwong; Chau, H. F. (1999). "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances" (https://www.jstor.org/stable/pdf/2896688.pdf) (PDF). *Science*. **283** (5410): 2050–2056. arXiv:quant-ph/9803006 (https://arxiv.org/abs/quant-ph/9803006). Bibcode:1999Sci...283.2050L (https://ui.adsabs.harvard.edu/abs/1999Sci...283.2050L). doi:10.1126/science.283.5410.2050 (https://doi.org/10.1126%2Fscience.283.5410.2050). JSTOR 2896688 (https://www.jstor.org/stable/2896688). PMID 10092221 (https://pubmed.ncbi.nlm.nih.gov/10092221). S2CID 2948183 (https://api.semanticscholar.org/CorpusID:2948183).
12. Pirandola, S.; García-Patrón, R.; Braunstein, S. L.; Lloyd, S. (2009). "Direct and Reverse Secret-Key Capacities of a Quantum Channel". *Physical Review Letters*. **102** (5): 050503. arXiv:0809.3273 (https://arxiv.org/abs/0809.3273). Bibcode:2009PhRvL.102e0503P (https://ui.adsabs.harvard.edu/abs/2009PhRvL.102e0503P). doi:10.1103/PhysRevLett.102.050503 (https://doi.org/10.1103%2FPhysRevLett.102.050503). PMID 19257494 (https://pubmed.ncbi.nlm.nih.gov/19257494). S2CID 665165 (https://api.semanticscholar.org/CorpusID:665165).

13. Takeoka, Masahiro; Guha, Saikat; Wilde, Mark M. (2014). "Fundamental rate-loss tradeoff for optical quantum key distribution". *Nature Communications*. **5**: 5235. arXiv:1504.06390 (https://arxiv.org/abs/1504.06390). Bibcode:2014NatCo...5.5235T (https://ui.adsabs.harvard.edu/abs/2014NatCo...5.5235T). doi:10.1038/ncomms6235 (https://doi.org/10.1038%2Fncomms6235). PMID 25341406 (https://pubmed.ncbi.nlm.nih.gov/25341406). S2CID 20580923 (https://api.semanticscholar.org/CorpusID:20580923).
14. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. (2017). "Fundamental limits of repeaterless quantum communications" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5414096). *Nature Communications*. **8**: 15043. arXiv:1510.08863 (https://arxiv.org/abs/1510.08863). Bibcode:2017NatCo...815043P (https://ui.adsabs.harvard.edu/abs/2017NatCo...815043P). doi:10.1038/ncomms15043 (https://doi.org/10.1038%2Fncomms15043). PMC 5414096 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5414096). PMID 28443624 (https://pubmed.ncbi.nlm.nih.gov/28443624).
15. Shields, A. J.; Dynes, J. F.; Yuan, Z. L.; Lucamarini, M. (May 2018). "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters". *Nature*. **557** (7705): 400–403. arXiv:1811.06826 (https://arxiv.org/abs/1811.06826). Bibcode:2018Natur.557..400L (https://ui.adsabs.harvard.edu/abs/2018Natur.557..400L). doi:10.1038/s41586-018-0066-6 (https://doi.org/10.1038%2Fs41586-018-0066-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 29720656 (https://pubmed.ncbi.nlm.nih.gov/29720656). S2CID 21698666 (https://api.semanticscholar.org/CorpusID:21698666).
16. Pirandola, S. (2019). "End-to-end capacities of a quantum communication network". *Communications Physics*. **2** (1): 51. arXiv:1601.00966 (https://arxiv.org/abs/1601.00966). Bibcode:2019CmPhy...2...51P (https://ui.adsabs.harvard.edu/abs/2019CmPhy...2...51P). doi:10.1038/s42005-019-0147-3 (https://doi.org/10.1038%2Fs42005-019-0147-3). S2CID 170078611 (https://api.semanticscholar.org/CorpusID:170078611).
17. Minder, Mariella; Pittaluga, Mirko; Roberts, George; Lucamarini, Marco; Dynes, James F.; Yuan, Zhiliang; Shields, Andrew J. (February 2019). "Experimental quantum key distribution beyond the repeaterless secret key capacity". *Nature Photonics*. **13** (5): 334–338. arXiv:1910.01951 (https://arxiv.org/abs/1910.01951). Bibcode:2019NaPho..13..334M (https://ui.adsabs.harvard.edu/abs/2019NaPho..13..334M). doi:10.1038/s41566-019-0377-7 (https://doi.org/10.1038%2Fs41566-019-0377-7). S2CID 126717712 (https://api.semanticscholar.org/CorpusID:126717712).
18. Wang, Xiang-Bin; Yu, Zong-Wen; Hu, Xiao-Long (2018). "Twin-field quantum key distribution with large misalignment error". *Physical Review A*. **98** (6): 062323. arXiv:1805.09222 (https://arxiv.org/abs/1805.09222). Bibcode:2018PhRvA..98f2323W (https://ui.adsabs.harvard.edu/abs/2018PhRvA..98f2323W). doi:10.1103/PhysRevA.98.062323 (https://doi.org/10.1103%2FPhysRevA.98.062323). S2CID 51204011 (https://api.semanticscholar.org/CorpusID:51204011).
19. Xu, Hai; Yu, Zong-Wen; Hu, Xiao-Long; Wang, Xiang-Bin (2020). "Improved results for sending-or-not-sending twin-field quantun key distribution: breaking the absolute limit of repeaterless key rate". *Physical Review A*. **101**: 042330. arXiv:1904.06331 (https://arxiv.org/abs/1904.06331). doi:10.1103/PhysRevA.101.042330 (https://doi.org/10.1103%2FPhysRevA.101.042330). S2CID 219003338 (https://api.semanticscholar.org/CorpusID:219003338).
20. Cui, C.; Yin, A.-Q.; Wang, R.; Chen, W.; Wang, S.; Guo, G.-C.; Han, Z.-F. (2019). "Twin-Field Quantum Key Distribution without Phase Postselection". *Physical Review Applied*. **11** (3): 034053. arXiv:1807.02334 (https://arxiv.org/abs/1807.02334). Bibcode:2019PhRvP..11c4053C (https://ui.adsabs.harvard.edu/abs/2019PhRvP..11c4053C). doi:10.1103/PhysRevApplied.11.034053 (https://doi.org/10.1103%2FPhysRevApplied.11.034053). S2CID 53624575 (https://api.semanticscholar.org/CorpusID:53624575).

21. Mayers, Dominic (1997). "Unconditionally Secure Quantum Bit Commitment is Impossible". *Physical Review Letters*. **78** (17): 3414–3417. arXiv:quant-ph/9605044 (https://arxiv.org/abs/quant-ph/9605044). Bibcode:1997PhRvL..78.3414M (https://ui.adsabs.harvard.edu/abs/1997PhRvL..78.3414M). CiteSeerX 10.1.1.251.5550 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.251.5550). doi:10.1103/PhysRevLett.78.3414 (https://doi.org/10.1103%2FPhysRevLett.78.3414). S2CID 14522232 (https://api.semanticscholar.org/CorpusID:14522232).
22. Lo, H.-K.; Chau, H. (1997). "Is Quantum Bit Commitment Really Possible?". *Physical Review Letters*. **78** (17): 3410. arXiv:quant-ph/9603004 (https://arxiv.org/abs/quant-ph/9603004). Bibcode:1997PhRvL..78.3410L (https://ui.adsabs.harvard.edu/abs/1997PhRvL..78.3410L). doi:10.1103/PhysRevLett.78.3410 (https://doi.org/10.1103%2FPhysRevLett.78.3410). S2CID 3264257 (https://api.semanticscholar.org/CorpusID:3264257).
23. Lo, H.-K.; Chau, H. (1998). "Why quantum bit commitment and ideal quantum coin tossing are impossible". *Physica D: Nonlinear Phenomena*. **120** (1–2): 177–187. arXiv:quant-ph/9711065 (https://arxiv.org/abs/quant-ph/9711065). Bibcode:1998PhyD..120..177L (https://ui.adsabs.harvard.edu/abs/1998PhyD..120..177L). doi:10.1016/S0167-2789(98)00053-0 (https://doi.org/10.1016%2FS0167-2789%2898%2900053-0). S2CID 14378275 (https://api.semanticscholar.org/CorpusID:14378275).
24. Lo, H.-K. (1997). "Insecurity of quantum secure computations". *Physical Review A*. **56** (2): 1154–1162. arXiv:quant-ph/9611031 (https://arxiv.org/abs/quant-ph/9611031). Bibcode:1997PhRvA..56.1154L (https://ui.adsabs.harvard.edu/abs/1997PhRvA..56.1154L). doi:10.1103/PhysRevA.56.1154 (https://doi.org/10.1103%2FPhysRevA.56.1154). S2CID 17813922 (https://api.semanticscholar.org/CorpusID:17813922).
25. Kent, A. (1999). "Unconditionally Secure Bit Commitment". *Physical Review Letters*. **83** (7): 1447–1450. arXiv:quant-ph/9810068 (https://arxiv.org/abs/quant-ph/9810068). Bibcode:1999PhRvL..83.1447K (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83.1447K). doi:10.1103/PhysRevLett.83.1447 (https://doi.org/10.1103%2FPhysRevLett.83.1447). S2CID 8823466 (https://api.semanticscholar.org/CorpusID:8823466).
26. Kent, A. (1999). "Coin Tossing is Strictly Weaker than Bit Commitment". *Physical Review Letters*. **83** (25): 5382–5384. arXiv:quant-ph/9810067 (https://arxiv.org/abs/quant-ph/9810067). Bibcode:1999PhRvL..83.5382K (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83.5382K). doi:10.1103/PhysRevLett.83.5382 (https://doi.org/10.1103%2FPhysRevLett.83.5382). S2CID 16764407 (https://api.semanticscholar.org/CorpusID:16764407).
27. Stuart Mason Dambort (26 March 2014). "Heads or tails: Experimental quantum coin flipping cryptography performs better than classical protocols" (https://phys.org/news/2014-05-tails-experimental-quantum-coin-flipping.html). *Phys.org*. Archived (https://web.archive.org/web/20170325025154/https://phys.org/news/2014-05-tails-experimental-quantum-coin-flipping.html) from the original on 25 March 2017.
28. Doescher, C.; Keyl, M. (2002). "An introduction to quantum coin-tossing". arXiv:quant-ph/0206088 (https://arxiv.org/abs/quant-ph/0206088).
29. Pappa, Anna; Jouguet, Paul; Lawson, Thomas; Chailloux, André; Legré, Matthieu; Trinkler, Patrick; Kerenidis, Iordanis; Diamanti, Eleni (24 April 2014). "Experimental plug and play quantum coin flipping" (https://www.nature.com/articles/ncomms4717). *Nature Communications*. **5** (1): 3717. arXiv:1306.3368 (https://arxiv.org/abs/1306.3368). Bibcode:2014NatCo...5.3717P (https://ui.adsabs.harvard.edu/abs/2014NatCo...5.3717P). doi:10.1038/ncomms4717 (https://doi.org/10.1038%2Fncomms4717). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMID 24758868 (https://pubmed.ncbi.nlm.nih.gov/24758868). S2CID 205325088 (https://api.semanticscholar.org/CorpusID:205325088).
30. Ambainis, Andris (1 March 2004). "A new protocol and lower bounds for quantum coin flipping" (https://www.sciencedirect.com/science/article/pii/S0022000003001417). *Journal of Computer and System Sciences*. **68** (2): 398–416. arXiv:quant-ph/0204022 (https://arxiv.org/abs/quant-ph/0204022). doi:10.1016/j.jcss.2003.07.010 (https://doi.org/10.1016%2Fj.jcss.2003.07.010). ISSN 0022-0000 (https://search.worldcat.org/issn/0022-0000).

31. "Heads or tails: Experimental quantum coin flipping cryptography performs better than classical protocols" (https://phys.org/news/2014-05-tails-experimental-quantum-coin-flipping.html). *phys.org*. Retrieved 18 October 2020.
32. Bennett, Charles H.; Brassard, Gilles (4 December 2014). "Quantum cryptography: Public key distribution and coin tossing" (https://doi.org/10.1016%2Fj.tcs.2014.05.025). *Theoretical Computer Science*. **560**: 7–11. arXiv:2003.06557 (https://arxiv.org/abs/2003.06557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025). ISSN 0304-3975 (https://search.worldcat.org/issn/0304-3975). S2CID 27022972 (https://api.semanticscholar.org/CorpusID:27022972).
33. Crépeau, Claude; Joe, Kilian (1988). *Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract)*. FOCS 1988. IEEE. pp. 42–52.
34. Kilian, Joe (1988). *Founding cryptography on oblivious transfer* (https://web.archive.org/web/20041224234245/http://external.nj.nec.com/homepages/joe/collected-papers/Kil88b.ps). STOC 1988. ACM. pp. 20–31. Archived from the original (http://external.nj.nec.com/homepages/joe/collected-papers/Kil88b.ps) on 24 December 2004.
35. Brassard, Gilles; Claude, Crépeau; Jozsa, Richard; Langlois, Denis (1993). *A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties*. FOCS 1993. IEEE. pp. 362–371.
36. Lunghi, T.; Kaniewski, J.; Bussières, F.; Houlmann, R.; Tomamichel, M.; Kent, A.; Gisin, N.; Wehner, S.; Zbinden, H. (2013). "Experimental Bit Commitment Based on Quantum Communication and Special Relativity". *Physical Review Letters*. **111** (18): 180504. arXiv:1306.4801 (https://arxiv.org/abs/1306.4801). Bibcode:2013PhRvL.111r0504L (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111r0504L). doi:10.1103/PhysRevLett.111.180504 (https://doi.org/10.1103%2FPhysRevLett.111.180504). PMID 24237497 (https://pubmed.ncbi.nlm.nih.gov/24237497). S2CID 15916727 (https://api.semanticscholar.org/CorpusID:15916727).
37. Wang, Ming-Qiang; Wang, Xue; Zhan, Tao (2018). "Unconditionally secure multi-party quantum commitment scheme". *Quantum Information Processing*. **17** (2): 31. Bibcode:2018QuIP...17...31W (https://ui.adsabs.harvard.edu/abs/2018QuIP...17...31W). doi:10.1007/s11128-017-1804-7 (https://doi.org/10.1007%2Fs11128-017-1804-7). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 3603337 (https://api.semanticscholar.org/CorpusID:3603337).
38. Nikolopoulos, Georgios M. (2019). "Optical scheme for cryptographic commitments with physical unclonable keys" (https://doi.org/10.1364/OE.27.029367). *Optics Express*. **27** (20): 29367–29379. arXiv:1909.13094 (https://arxiv.org/abs/1909.13094). Bibcode:2019OExpr..2729367N (https://ui.adsabs.harvard.edu/abs/2019OExpr..2729367N). doi:10.1364/OE.27.029367 (https://doi.org/10.1364%2FOE.27.029367). PMID 31684673 (https://pubmed.ncbi.nlm.nih.gov/31684673). S2CID 203593129 (https://api.semanticscholar.org/CorpusID:203593129). Retrieved 13 November 2020.
39. Damgård, Ivan; Fehr, Serge; Salvail, Louis; Schaffner, Christian (2005). *Cryptography in the Bounded Quantum-Storage Model*. FOCS 2005. IEEE. pp. 449–458. arXiv:quant-ph/0508222 (https://arxiv.org/abs/quant-ph/0508222).
40. Wehner, Stephanie; Schaffner, Christian; Terhal, Barbara M. (2008). "Cryptography from Noisy Storage". *Physical Review Letters*. **100** (22): 220502. arXiv:0711.2895 (https://arxiv.org/abs/0711.2895). Bibcode:2008PhRvL.100v0502W (https://ui.adsabs.harvard.edu/abs/2008PhRvL.100v0502W). doi:10.1103/PhysRevLett.100.220502 (https://doi.org/10.1103%2FPhysRevLett.100.220502). PMID 18643410 (https://pubmed.ncbi.nlm.nih.gov/18643410). S2CID 2974264 (https://api.semanticscholar.org/CorpusID:2974264).
41. Doescher, C.; Keyl, M.; Wullschleger, Jürg (2009). "Unconditional security from noisy quantum storage". *IEEE Transactions on Information Theory*. **58** (3): 1962–1984. arXiv:0906.1030 (https://arxiv.org/abs/0906.1030). doi:10.1109/TIT.2011.2177772 (https://doi.org/10.1109%2FTIT.2011.2177772). S2CID 12500084 (https://api.semanticscholar.org/CorpusID:12500084).

42. Cachin, Christian; Crépeau, Claude; Marcil, Julien (1998). *Oblivious Transfer with a Memory-Bounded Receiver*. FOCS 1998. IEEE. pp. 493–502.
43. Dziembowski, Stefan; Ueli, Maurer (2004). *On Generating the Initial Key in the Bounded-Storage Model* (https://www.crypto.ethz.ch/publications/files/DziMau04b.pdf) (PDF). Eurocrypt 2004. LNCS. Vol. 3027. Springer. pp. 126–137. Archived (https://web.archive.org/web/20200311235001/https://www.crypto.ethz.ch/publications/files/DziMau04b.pdf) (PDF) from the original on 11 March 2020. Retrieved 11 March 2020.
44. Chandran, Nishanth; Moriarty, Ryan; Goyal, Vipul; Ostrovsky, Rafail (2009). "Position-Based Cryptography" (http://eprint.iacr.org/2009/364). *Cryptology ePrint Archive*.
45. US 7075438 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US7075438), issued 2006-07-11
46. Malaney, Robert (2010). "Location-dependent communications using quantum entanglement". *Physical Review A*. **81** (4): 042319. arXiv:1003.0949 (https://arxiv.org/abs/1003.0949). Bibcode:2010PhRvA..81d2319M (https://ui.adsabs.harvard.edu/abs/2010PhRvA..81d2319M). doi:10.1103/PhysRevA.81.042319 (https://doi.org/10.1103%2FPhysRevA.81.042319). S2CID 118704298 (https://api.semanticscholar.org/CorpusID:118704298).
47. Malaney, Robert (2010). "Quantum Location Verification in Noisy Channels". *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE Global Telecommunications Conference GLOBECOM 2010. pp. 1–6. arXiv:1004.4689 (https://arxiv.org/abs/1004.4689). doi:10.1109/GLOCOM.2010.5684009 (https://doi.org/10.1109%2FGLOCOM.2010.5684009). ISBN 978-1-4244-5636-9.
48. Doescher, C.; Keyl, M.; Spiller, Timothy P. (2011). "Quantum Tagging: Authenticating Location via Quantum Information and Relativistic Signalling Constraints". *Physical Review A*. **84** (1): 012326. arXiv:1008.2147 (https://arxiv.org/abs/1008.2147). Bibcode:2011PhRvA..84a2326K (https://ui.adsabs.harvard.edu/abs/2011PhRvA..84a2326K). doi:10.1103/PhysRevA.84.012326 (https://doi.org/10.1103%2FPhysRevA.84.012326). S2CID 1042757 (https://api.semanticscholar.org/CorpusID:1042757).
49. Lau, Hoi-Kwan; Lo, Hoi-Kwong (2010). "Insecurity of position-based quantum-cryptography protocols against entanglement attacks". *Physical Review A*. **83** (1): 012322. arXiv:1009.2256 (https://arxiv.org/abs/1009.2256). Bibcode:2011PhRvA..83a2322L (https://ui.adsabs.harvard.edu/abs/2011PhRvA..83a2322L). doi:10.1103/PhysRevA.83.012322 (https://doi.org/10.1103%2FPhysRevA.83.012322). S2CID 17022643 (https://api.semanticscholar.org/CorpusID:17022643).
50. Doescher, C.; Keyl, M.; Fehr, Serge; Gelles, Ran; Goyal, Vipul; Ostrovsky, Rafail; Schaffner, Christian (2010). "Position-Based Quantum Cryptography: Impossibility and Constructions". *SIAM Journal on Computing*. **43**: 150–178. arXiv:1009.2490 (https://arxiv.org/abs/1009.2490). Bibcode:2010arXiv1009.2490B (https://ui.adsabs.harvard.edu/abs/2010arXiv1009.2490B). doi:10.1137/130913687 (https://doi.org/10.1137%2F130913687). S2CID 220613220 (https://api.semanticscholar.org/CorpusID:220613220).
51. Beigi, Salman; König, Robert (2011). "Simplified instantaneous non-local quantum computation with applications to position-based cryptography". *New Journal of Physics*. **13** (9): 093036. arXiv:1101.1065 (https://arxiv.org/abs/1101.1065). Bibcode:2011NJPh...13i3036B (https://ui.adsabs.harvard.edu/abs/2011NJPh...13i3036B). doi:10.1088/1367-2630/13/9/093036 (https://doi.org/10.1088%2F1367-2630%2F13%2F9%2F093036). S2CID 27648088 (https://api.semanticscholar.org/CorpusID:27648088).
52. Malaney, Robert (2016). "The Quantum Car". *IEEE Wireless Communications Letters*. **5** (6): 624–627. arXiv:1512.03521 (https://arxiv.org/abs/1512.03521). doi:10.1109/LWC.2016.2607740 (https://doi.org/10.1109%2FLWC.2016.2607740). S2CID 2483729 (https://api.semanticscholar.org/CorpusID:2483729).

53. Radanliev, Petar (October 2023). "Red Teaming Generative AI/NLP, the BB84 quantum cryptography protocol and the NIST-approved Quantum-Resistant Cryptographic Algorithms" (https://ora.ox.ac.uk/objects/uuid:45d125d9-2ae5-4dff-9806-6ea4c512c6b1/download_file?file_format=application%2Fpdf&safe_filename=Radanliev_et_al_2023_Red_Teaming_Generative.pdf&type_of_work=Internet+publication). *University of Oxford*. arXiv:2310.04425 (https://arxiv.org/abs/2310.04425).
54. Mayers, Dominic; Yao, Andrew C.-C. (1998). *Quantum Cryptography with Imperfect Apparatus*. IEEE Symposium on Foundations of Computer Science (FOCS). arXiv:quant-ph/9809039 (https://arxiv.org/abs/quant-ph/9809039). Bibcode:1998quant.ph..9039M (https://ui.adsabs.harvard.edu/abs/1998quant.ph..9039M).
55. Colbeck, Roger (December 2006). "Chapter 5". *Quantum And Relativistic Protocols For Secure Multi-Party Computation* (Thesis). University of Cambridge. arXiv:0911.3814 (https://arxiv.org/abs/0911.3814).
56. Vazirani, Umesh; Vidick, Thomas (2014). "Fully Device-Independent Quantum Key Distribution". *Physical Review Letters*. **113** (2): 140501. arXiv:1403.3830 (https://arxiv.org/abs/1403.3830). Bibcode:2014PhRvL.113b0501A (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113b0501A). doi:10.1103/PhysRevLett.113.020501 (https://doi.org/10.1103%2FPhysRevLett.113.020501). PMID 25062151 (https://pubmed.ncbi.nlm.nih.gov/25062151). S2CID 23057977 (https://api.semanticscholar.org/CorpusID:23057977).
57. Miller, Carl; Shi, Yaoyun (2014). "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices". *Journal of the ACM*. **63** (4): 33. arXiv:1402.0489 (https://arxiv.org/abs/1402.0489). Bibcode:2014arXiv1402.0489M (https://ui.adsabs.harvard.edu/abs/2014arXiv1402.0489M).
58. Miller, Carl; Shi, Yaoyun (2017). "Universal security for randomness expansion". *SIAM Journal on Computing*. **46** (4): 1304–1335. arXiv:1411.6608 (https://arxiv.org/abs/1411.6608). doi:10.1137/15M1044333 (https://doi.org/10.1137%2F15M1044333). S2CID 6792482 (https://api.semanticscholar.org/CorpusID:6792482).
59. Chung, Kai-Min; Shi, Yaoyun; Wu, Xiaodi (2014). "Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions". arXiv:1402.4797 (https://arxiv.org/abs/1402.4797) [quant-ph (https://arxiv.org/archive/quant-ph)].
60. Arnon-Friedman, Rotem; Dupuis, Frédéric; Fawzi, Omar; Renner, Renato; Vidick, Thomas (31 January 2018). "Practical device-independent quantum cryptography via entropy accumulation" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5792631). *Nature Communications*. **9** (1): 459. Bibcode:2018NatCo...9..459A (https://ui.adsabs.harvard.edu/abs/2018NatCo...9..459A). doi:10.1038/s41467-017-02307-4 (https://doi.org/10.1038%2Fs41467-017-02307-4). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 5792631 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5792631). PMID 29386507 (https://pubmed.ncbi.nlm.nih.gov/29386507).
61. Daniel J. Bernstein (2009). "Introduction to post-quantum cryptography" (http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf) (PDF). *Post-Quantum Cryptography*.
62. Daniel J. Bernstein (17 May 2009). Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? (http://cr.yp.to/hash/collisioncost-20090823.pdf) (PDF) (Report). Archived (https://web.archive.org/web/20170825091116/https://cr.yp.to/hash/collisioncost-20090823.pdf) (PDF) from the original on 25 August 2017.
63. "Post-quantum cryptography" (http://pqcrypto.org/). Archived (https://web.archive.org/web/20110717174032/http://pqcrypto.org/) from the original on 17 July 2011. Retrieved 29 August 2010.
64. Bernstein, Daniel J.; Buchmann, Johannes; Dahmen, Erik, eds. (2009). *Post-quantum cryptography*. Springer. ISBN 978-3-540-88701-0.

65. Watrous, John (2009). "Zero-Knowledge against Quantum Attacks". *SIAM Journal on Computing*. **39** (1): 25–58. arXiv:quant-ph/0511020 (https://arxiv.org/abs/quant-ph/0511020). CiteSeerX 10.1.1.190.2789 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.190.2789). doi:10.1137/060670997 (https://doi.org/10.1137%2F060670997).
66. "NSA Suite B Cryptography" (https://web.archive.org/web/20160101091229/https://www.nsa.gov/ia/programs/suiteb_cryptography/). Archived from the original (https://www.nsa.gov/ia/programs/suiteb_cryptography/) on 1 January 2016. Retrieved 29 December 2015.
67. "Quantum Resistant Public Key Exchange: The Supersingular Isogenous Diffie-Hellman Protocol – CoinFabrik Blog" (http://blog.coinfabrik.com/quantum-resistant-public-key-exchange-the-supersingular-isogenous-diffie-hellman-protocol/). *blog.coinfabrik.com*. 13 October 2016. Archived (https://web.archive.org/web/20170202071502/http://blog.coinfabrik.com/quantum-resistant-public-key-exchange-the-supersingular-isogenous-diffie-hellman-protocol/) from the original on 2 February 2017. Retrieved 24 January 2017.
68. Thapliyal, K.; Pathak, A. (2018). "Kak's three-stage protocol of secure quantum communication revisited". *Quantum Information Processing*. **17** (9): 229. arXiv:1803.02157 (https://arxiv.org/abs/1803.02157). Bibcode:2018QuIP...17..229T (https://ui.adsabs.harvard.edu/abs/2018QuIP...17..229T). doi:10.1007/s11128-018-2001-z (https://doi.org/10.1007%2Fs11128-018-2001-z). S2CID 52009384 (https://api.semanticscholar.org/CorpusID:52009384).
69. Nikolopoulos, Georgios M.; Fischlin, Marc (2020). "Information-Theoretically Secure Data Origin Authentication with Quantum and Classical Resources" (https://doi.org/10.3390%2Fcryptography4040031). *Cryptography*. **4** (4): 31. arXiv:2011.06849 (https://arxiv.org/abs/2011.06849). doi:10.3390/cryptography4040031 (https://doi.org/10.3390%2Fcryptography4040031). S2CID 226956062 (https://api.semanticscholar.org/CorpusID:226956062).
70. Doescher, C.; Keyl, M. (2001). "Quantum Digital Signatures". arXiv:quant-ph/0105032 (https://arxiv.org/abs/quant-ph/0105032).
71. Collins, Robert J.; Donaldson, Ross J.; Dunjko, Vedran; Wallden, Petros; Clarke, Patrick J.; Andersson, Erika; Jeffers, John; Buller, Gerald S. (2014). "Realization of Quantum Digital Signatures without the Requirement of Quantum Memory". *Physical Review Letters*. **113** (4): 040502. arXiv:1311.5760 (https://arxiv.org/abs/1311.5760). Bibcode:2014PhRvL.113d0502C (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113d0502C). doi:10.1103/PhysRevLett.113.040502 (https://doi.org/10.1103%2FPhysRevLett.113.040502). PMID 25105603 (https://pubmed.ncbi.nlm.nih.gov/25105603). S2CID 23925266 (https://api.semanticscholar.org/CorpusID:23925266).
72. Kawachi, Akinori; Koshiba, Takeshi; Nishimura, Harumichi; Yamakami, Tomoyuki (2011). "Computational Indistinguishability Between Quantum States and its Cryptographic Application". *Journal of Cryptology*. **25** (3): 528–555. arXiv:quant-ph/0403069 (https://arxiv.org/abs/quant-ph/0403069). CiteSeerX 10.1.1.251.6055 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.251.6055). doi:10.1007/s00145-011-9103-4 (https://doi.org/10.1007%2Fs00145-011-9103-4). S2CID 6340239 (https://api.semanticscholar.org/CorpusID:6340239).
73. Kabashima, Yoshiyuki; Murayama, Tatsuto; Saad, David (2000). "Cryptographical Properties of Ising Spin Systems". *Physical Review Letters*. **84** (9): 2030–2033. arXiv:cond-mat/0002129 (https://arxiv.org/abs/cond-mat/0002129). Bibcode:2000PhRvL..84.2030K (https://ui.adsabs.harvard.edu/abs/2000PhRvL..84.2030K). doi:10.1103/PhysRevLett.84.2030 (https://doi.org/10.1103%2FPhysRevLett.84.2030). PMID 11017688 (https://pubmed.ncbi.nlm.nih.gov/11017688). S2CID 12883829 (https://api.semanticscholar.org/CorpusID:12883829).
74. Nikolopoulos, Georgios M. (2008). "Applications of single-qubit rotations in quantum public-key cryptography". *Physical Review A*. **77** (3): 032348. arXiv:0801.2840 (https://arxiv.org/abs/0801.2840). Bibcode:2008PhRvA..77c2348N (https://ui.adsabs.harvard.edu/abs/2008PhRvA..77c2348N). doi:10.1103/PhysRevA.77.032348 (https://doi.org/10.1103%2FPhysRevA.77.032348). S2CID 119097757 (https://api.semanticscholar.org/CorpusID:119097757).

75. Nikolopoulos, Georgios M.; Ioannou, Lawrence M. (2009). "Deterministic quantum-public-key encryption: Forward search attack and randomization". *Physical Review A*. **79** (4): 042327. arXiv:0903.4744 (https://arxiv.org/abs/0903.4744). Bibcode:2009PhRvA..79d2327N (https://ui.adsabs.harvard.edu/abs/2009PhRvA..79d2327N). doi:10.1103/PhysRevA.79.042327 (https://doi.org/10.1103%2FPhysRevA.79.042327). S2CID 118425296 (https://api.semanticscholar.org/CorpusID:118425296).
76. Seyfarth, U.; Nikolopoulos, G. M.; Alber, G. (2012). "Symmetries and security of a quantum-public-key encryption based on single-qubit rotations". *Physical Review A*. **85** (2): 022342. arXiv:1202.3921 (https://arxiv.org/abs/1202.3921). Bibcode:2012PhRvA..85b2342S (https://ui.adsabs.harvard.edu/abs/2012PhRvA..85b2342S). doi:10.1103/PhysRevA.85.022342 (https://doi.org/10.1103%2FPhysRevA.85.022342). S2CID 59467718 (https://api.semanticscholar.org/CorpusID:59467718).
77. Nikolopoulos, Georgios M.; Brougham, Thomas (11 July 2016). "Decision and function problems based on boson sampling" (https://link.aps.org/doi/10.1103/PhysRevA.94.012315). *Physical Review A*. **94** (1): 012315. arXiv:1607.02987 (https://arxiv.org/abs/1607.02987). Bibcode:2016PhRvA..94a2315N (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94a2315N). doi:10.1103/PhysRevA.94.012315 (https://doi.org/10.1103%2FPhysRevA.94.012315). S2CID 5311008 (https://api.semanticscholar.org/CorpusID:5311008).
78. Nikolopoulos, Georgios M. (13 July 2019). "Cryptographic one-way function based on boson sampling" (https://doi.org/10.1007/s11128-019-2372-9). *Quantum Information Processing*. **18** (8): 259. arXiv:1907.01788 (https://arxiv.org/abs/1907.01788). Bibcode:2019QuIP...18..259N (https://ui.adsabs.harvard.edu/abs/2019QuIP...18..259N). doi:10.1007/s11128-019-2372-9 (https://doi.org/10.1007%2Fs11128-019-2372-9). ISSN 1573-1332 (https://search.worldcat.org/issn/1573-1332). S2CID 195791867 (https://api.semanticscholar.org/CorpusID:195791867).
79. Buhrman, Harry; Cleve, Richard; Watrous, John; De Wolf, Ronald (2001). "Quantum Fingerprinting". *Physical Review Letters*. **87** (16): 167902. arXiv:quant-ph/0102001 (https://arxiv.org/abs/quant-ph/0102001). Bibcode:2001PhRvL..87p7902B (https://ui.adsabs.harvard.edu/abs/2001PhRvL..87p7902B). doi:10.1103/PhysRevLett.87.167902 (https://doi.org/10.1103%2FPhysRevLett.87.167902). PMID 11690244 (https://pubmed.ncbi.nlm.nih.gov/11690244). S2CID 1096490 (https://api.semanticscholar.org/CorpusID:1096490).
80. Nikolopoulos, Georgios M.; Diamanti, Eleni (10 April 2017). "Continuous-variable quantum authentication of physical unclonable keys" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5385567). *Scientific Reports*. **7** (1): 46047. arXiv:1704.06146 (https://arxiv.org/abs/1704.06146). Bibcode:2017NatSR...746047N (https://ui.adsabs.harvard.edu/abs/2017NatSR...746047N). doi:10.1038/srep46047 (https://doi.org/10.1038%2Fsrep46047). ISSN 2045-2322 (https://search.worldcat.org/issn/2045-2322). PMC 5385567 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5385567). PMID 28393853 (https://pubmed.ncbi.nlm.nih.gov/28393853).
81. Nikolopoulos, Georgios M. (22 January 2018). "Continuous-variable quantum authentication of physical unclonable keys: Security against an emulation attack" (https://link.aps.org/doi/10.1103/PhysRevA.97.012324). *Physical Review A*. **97** (1): 012324. arXiv:1801.07434 (https://arxiv.org/abs/1801.07434). Bibcode:2018PhRvA..97a2324N (https://ui.adsabs.harvard.edu/abs/2018PhRvA..97a2324N). doi:10.1103/PhysRevA.97.012324 (https://doi.org/10.1103%2FPhysRevA.97.012324). S2CID 119486945 (https://api.semanticscholar.org/CorpusID:119486945).
82. Fladung, Lukas; Nikolopoulos, Georgios M.; Alber, Gernot; Fischlin, Marc (2019). "Intercept-Resend Emulation Attacks against a Continuous-Variable Quantum Authentication Protocol with Physical Unclonable Keys" (https://doi.org/10.3390%2Fcryptography3040025). *Cryptography*. **3** (4): 25. arXiv:1910.11579 (https://arxiv.org/abs/1910.11579). doi:10.3390/cryptography3040025 (https://doi.org/10.3390%2Fcryptography3040025). S2CID 204901444 (https://api.semanticscholar.org/CorpusID:204901444).

83. Barbosa, Geraldo A.; Corndorf, Eric; Kumar, Prem; Yuen, Horace P. (2 June 2003). "Secure Communication Using Mesoscopic Coherent States" (https://doi.org/10.1103/PhysRevLett.90.227901). *Physical Review Letters*. **90** (22): 227901. arXiv:quant-ph/0212018 (https://arxiv.org/abs/quant-ph/0212018). Bibcode:2003PhRvL..90v7901B (https://ui.adsabs.harvard.edu/abs/2003PhRvL..90v7901B). doi:10.1103/PhysRevLett.90.227901 (https://doi.org/10.1103%2FPhysRevLett.90.227901). PMID 12857341 (https://pubmed.ncbi.nlm.nih.gov/12857341). S2CID 12720233 (https://api.semanticscholar.org/CorpusID:12720233).
84. Yuen, H. P. (31 July 2009). *Physical Cryptography: A New Approach to Key Generation and Direct Encryption* (https://apps.dtic.mil/sti/pdfs/ADA512847.pdf) (PDF) (PhD thesis).
85. Verma, Pramode K.; El Rifai, Mayssaa; Chan, K. W. Clifford (19 August 2018). "Secure Communication Based on Quantum Noise" (https://doi.org/10.1007/978-981-10-8618-2_4). *Multi-photon Quantum Secure Communication*. Signals and Communication Technology. pp. 85–95. doi:10.1007/978-981-10-8618-2_4 (https://doi.org/10.1007%2F978-981-10-8618-2_4). ISBN 978-981-10-8617-5. S2CID 56788374 (https://api.semanticscholar.org/CorpusID:56788374).
86. Takehisa, Iwakoshi (27 January 2020). "Analysis of Y00 Protocol Under Quantum Generalization of a Fast Correlation Attack: Toward Information-Theoretic Security" (https://doi.org/10.1109/ACCESS.2020.2969455). *IEEE Access*. **8**: 23417–23426. arXiv:2001.11150 (https://arxiv.org/abs/2001.11150). Bibcode:2020IEEEA...823417I (https://ui.adsabs.harvard.edu/abs/2020IEEEA...823417I). doi:10.1109/ACCESS.2020.2969455 (https://doi.org/10.1109%2FACCESS.2020.2969455). S2CID 210966407 (https://api.semanticscholar.org/CorpusID:210966407).
87. Hirota, Osamu; et al. (1 September 2010). "Getting around the Shannon limit of cryptography" (https://doi.org/10.1117/2.1201008.003069). *SPIE Newsroom*. doi:10.1117/2.1201008.003069 (https://doi.org/10.1117%2F2.1201008.003069).
88. Quan, Yu; et al. (30 March 2020). "Secure 100Gb/s IMDD transmission over 100 km SSMF enabled by quantum noise stream cipher and sparse RLS-Volterra equalizer" (https://doi.org/10.1109%2FACCESS.2020.2984330). *IEEE Access*. **8**: 63585–63594. Bibcode:2020IEEEA...863585Y (https://ui.adsabs.harvard.edu/abs/2020IEEEA...863585Y). doi:10.1109/ACCESS.2020.2984330 (https://doi.org/10.1109%2FACCESS.2020.2984330). S2CID 215816092 (https://api.semanticscholar.org/CorpusID:215816092).
89. Wyner, A. D. (October 1975). "The Wire-Tap Channel" (https://doi.org/10.1002/j.1538-7305.1975.tb02040.x). *Bell System Technical Journal*. **54** (8): 1355–1387. doi:10.1002/j.1538-7305.1975.tb02040.x (https://doi.org/10.1002%2Fj.1538-7305.1975.tb02040.x). S2CID 21512925 (https://api.semanticscholar.org/CorpusID:21512925).
90. Roy J., Glauber (15 June 1963). "The Quantum Theory of Optical Coherence" (https://doi.org/10.1103%2FPhysRev.130.2529). *Physical Review*. **130** (6): 2529–2539. Bibcode:1963PhRv..130.2529G (https://ui.adsabs.harvard.edu/abs/1963PhRv..130.2529G). doi:10.1103/PhysRev.130.2529 (https://doi.org/10.1103%2FPhysRev.130.2529).
91. E. C. G., Sudarshan (1 April 1963). "Equivalence of Semiclassical and Quantum Mechanical Descriptions of Statistical Light Beams" (https://doi.org/10.1103/PhysRevLett.10.277). *Physical Review Letters*. **10** (7): 277–279. Bibcode:1963PhRvL..10..277S (https://ui.adsabs.harvard.edu/abs/1963PhRvL..10..277S). doi:10.1103/PhysRevLett.10.277 (https://doi.org/10.1103%2FPhysRevLett.10.277).
92. Walls, D. F.; Milburn, G. J. (January 2008). *Quantum optics* (https://books.google.com/books?id=LiWsc3Nlf0kC). Springer. ISBN 9783540285731.
93. Hirota, Osamu; et al. (26 August 2005). "Quantum stream cipher by the Yuen 2000 protocol: Design and experiment by an intensity-modulation scheme" (https://doi.org/10.1103/PhysRevA.72.022335). *Physical Review A*. **72** (2): 022335. arXiv:quant-ph/0507043 (https://arxiv.org/abs/quant-ph/0507043). Bibcode:2005PhRvA..72b2335H (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72b2335H). doi:10.1103/PhysRevA.72.022335 (https://doi.org/10.1103%2FPhysRevA.72.022335). S2CID 118937168 (https://api.semanticscholar.org/CorpusID:118937168).

94. Yoshida, Masato; et al. (15 February 2021). "10 Tbit/s QAM Quantum Noise Stream Cipher Coherent Transmission Over 160 Km" (https://doi.org/10.1109/JLT.2020.3016693). *Journal of Lightwave Technology*. **39** (4): 1056–1063. Bibcode:2021JLwT...39.1056Y (https://ui.adsabs.harvard.edu/abs/2021JLwT...39.1056Y). doi:10.1109/JLT.2020.3016693 (https://doi.org/10.1109%2FJLT.2020.3016693). S2CID 225383926 (https://api.semanticscholar.org/CorpusID:225383926).
95. Futami, Fumio; et al. (March 2018). "Dynamic Routing of Y-00 Quantum Stream Cipher in Field-Deployed Dynamic Optical Path Network" (https://doi.org/10.1364/OFC.2018.Tu2G.5). *Optical Fiber Communication Conference*. pp. Tu2G.5. doi:10.1364/OFC.2018.Tu2G.5 (https://doi.org/10.1364%2FOFC.2018.Tu2G.5). ISBN 978-1-943580-38-5. S2CID 49185664 (https://api.semanticscholar.org/CorpusID:49185664).
96. Tanizawa, Ken; Futami, Fumio (2020). *Security-Enhanced 10,118-km Single-Channel 40-Gbit/s Transmission Using PSK Y-00 Quantum Stream Cipher* (https://doi.org/10.1109/ECOC48923.2020.9333304). pp. 1–4. doi:10.1109/ECOC48923.2020.9333304 (https://doi.org/10.1109%2FECOC48923.2020.9333304). ISBN 978-1-7281-7361-0. S2CID 231852229 (https://api.semanticscholar.org/CorpusID:231852229).
97. Tanizawa, Ken; Futami, Fumio (April 2020). "Quantum Noise-Assisted Coherent Radio-over-Fiber Cipher System for Secure Optical Fronthaul and Microwave Wireless Links" (https://doi.org/10.1109%2FJLT.2020.2987213). *Journal of Lightwave Technology*. **38** (16): 4244–4249. Bibcode:2020JLwT...38.4244T (https://ui.adsabs.harvard.edu/abs/2020JLwT...38.4244T). doi:10.1109/JLT.2020.2987213 (https://doi.org/10.1109%2FJLT.2020.2987213). S2CID 219095947 (https://api.semanticscholar.org/CorpusID:219095947).
98. Yuen, Horace P. (November 2009). "Key Generation: Foundations and a New Quantum Approach" (https://doi.org/10.1109/JSTQE.2009.2025698). *IEEE Journal of Selected Topics in Quantum Electronics*. **15** (6): 1630–1645. arXiv:0906.5241 (https://arxiv.org/abs/0906.5241). Bibcode:2009IJSTQ..15.1630Y (https://ui.adsabs.harvard.edu/abs/2009IJSTQ..15.1630Y). doi:10.1109/JSTQE.2009.2025698 (https://doi.org/10.1109%2FJSTQE.2009.2025698). S2CID 867791 (https://api.semanticscholar.org/CorpusID:867791).
99. Iwakoshi, Takehisa (5 June 2019). "Message-Falsification Prevention With Small Quantum Mask in Quaternary Y00 Protocol" (https://doi.org/10.1109%2FACCESS.2019.2921023). *IEEE Access*. **7**: 74482–74489. Bibcode:2019IEEEA...774482I (https://ui.adsabs.harvard.edu/abs/2019IEEEA...774482I). doi:10.1109/ACCESS.2019.2921023 (https://doi.org/10.1109%2FACCESS.2019.2921023). S2CID 195225370 (https://api.semanticscholar.org/CorpusID:195225370).
100. Nishioka, Tsuyoshi; et al. (21 June 2004). "How much security does Y-00 protocol provide us?" (https://doi.org/10.1016/j.physleta.2004.04.083). *Physics Letters A*. **327** (1): 28–32. arXiv:quant-ph/0310168 (https://arxiv.org/abs/quant-ph/0310168). Bibcode:2004PhLA..327...28N (https://ui.adsabs.harvard.edu/abs/2004PhLA..327...28N). doi:10.1016/j.physleta.2004.04.083 (https://doi.org/10.1016%2Fj.physleta.2004.04.083). S2CID 119069709 (https://api.semanticscholar.org/CorpusID:119069709).
101. Yuen, Horace P.; et al. (10 October 2005). "Comment on:'How much security does Y-00 protocol provide us?'[Phys. Lett. A 327 (2004) 28]" (https://doi.org/10.1016/j.physleta.2005.08.022). *Physics Letters A*. **346** (1–3): 1–6. Bibcode:2005PhLA..346....1Y (https://ui.adsabs.harvard.edu/abs/2005PhLA..346....1Y). doi:10.1016/j.physleta.2005.08.022 (https://doi.org/10.1016%2Fj.physleta.2005.08.022).
102. Nishioka, Tsuyoshi; et al. (10 October 2005). "Reply to:"Comment on:'How much security does Y-00 protocol provide us?'" [Phys. Lett. A 346 (2005) 1]" (https://doi.org/10.1016/j.physleta.2005.08.022). *Physics Letters A*. **346** (1–3). Bibcode:2005PhLA..346....1Y (https://ui.adsabs.harvard.edu/abs/2005PhLA..346....1Y). doi:10.1016/j.physleta.2005.08.022 (https://doi.org/10.1016%2Fj.physleta.2005.08.022).
103. Nair, Ranjith; et al. (13 September 2005). "Reply to:'Reply to:"Comment on:'How much security does Y-00 protocol provide us?'" ". arXiv:quant-ph/0509092 (https://arxiv.org/abs/quant-ph/0509092).

104. Donnet, Stéphane; et al. (21 August 2006). "Security of Y-00 under heterodyne measurement and fast correlation attack" (https://doi.org/10.1016/j.physleta.2006.04.002). *Physics Letters A*. **356** (6): 406–410. Bibcode:2006PhLA..356..406D (https://ui.adsabs.harvard.edu/abs/2006PhLA..356..406D). doi:10.1016/j.physleta.2006.04.002 (https://doi.org/10.1016%2Fj.physleta.2006.04.002).
105. Yuen, Horace P.; et al. (23 April 2007). "On the security of Y-00 under fast correlation and other attacks on the key" (https://doi.org/10.1016/j.physleta.2006.12.033). *Physics Letters A*. **364** (2): 112–116. arXiv:quant-ph/0608028 (https://arxiv.org/abs/quant-ph/0608028). Bibcode:2007PhLA..364..112Y (https://ui.adsabs.harvard.edu/abs/2007PhLA..364..112Y). doi:10.1016/j.physleta.2006.12.033 (https://doi.org/10.1016%2Fj.physleta.2006.12.033). S2CID 7824483 (https://api.semanticscholar.org/CorpusID:7824483).
106. Mihaljević, Miodrag J. (24 May 2007). "Generic framework for the secure Yuen 2000 quantum-encryption protocol employing the wire-tap channel approach" (https://doi.org/10.1103/PhysRevA.75.052334). *Physical Review A*. **75** (5): 052334. Bibcode:2007PhRvA..75e2334M (https://ui.adsabs.harvard.edu/abs/2007PhRvA..75e2334M). doi:10.1103/PhysRevA.75.052334 (https://doi.org/10.1103%2FPhysRevA.75.052334).
107. Shimizu, Tetsuya; et al. (27 March 2008). "Running key mapping in a quantum stream cipher by the Yuen 2000 protocol" (https://doi.org/10.1103/PhysRevA.77.034305). *Physical Review A*. **77** (3): 034305. Bibcode:2008PhRvA..77c4305S (https://ui.adsabs.harvard.edu/abs/2008PhRvA..77c4305S). doi:10.1103/PhysRevA.77.034305 (https://doi.org/10.1103%2FPhysRevA.77.034305).
108. Tregubov, P. A.; Trushechkin, A. S. (21 November 2020). "Quantum Stream Ciphers: Impossibility of Unconditionally Strong Algorithms". *Journal of Mathematical Sciences*. **252**: 90–103. doi:10.1007/s10958-020-05144-x (https://doi.org/10.1007%2Fs10958-020-05144-x). S2CID 254745640 (https://api.semanticscholar.org/CorpusID:254745640).
109. Iwakoshi, Takehisa (February 2021). "Security Evaluation of Y00 Protocol Based on Time-Translational Symmetry Under Quantum Collective Known-Plaintext Attacks" (https://doi.org/10.1109%2FACCESS.2021.3056494). *IEEE Access*. **9**: 31608–31617. Bibcode:2021IEEEA...931608I (https://ui.adsabs.harvard.edu/abs/2021IEEEA...931608I). doi:10.1109/ACCESS.2021.3056494 (https://doi.org/10.1109%2FACCESS.2021.3056494). S2CID 232072394 (https://api.semanticscholar.org/CorpusID:232072394).
110. Scarani, Valerio; Bechmann-Pasquinucci, Helle; Cerf, Nicolas J.; Dušek, Miloslav; Lütkenhaus, Norbert; Peev, Momtchil (29 September 2009). "The security of practical quantum key distribution" (https://dx.doi.org/10.1103/revmodphys.81.1301). *Reviews of Modern Physics*. **81** (3): 1301–1350. arXiv:0802.4155 (https://arxiv.org/abs/0802.4155). Bibcode:2009RvMP...81.1301S (https://ui.adsabs.harvard.edu/abs/2009RvMP...81.1301S). doi:10.1103/revmodphys.81.1301 (https://doi.org/10.1103%2Frevmodphys.81.1301). ISSN 0034-6861 (https://search.worldcat.org/issn/0034-6861). S2CID 15873250 (https://api.semanticscholar.org/CorpusID:15873250).
111. Zhao, Yi (2009). *Quantum cryptography in real-life applications: assumptions and security* (https://web.archive.org/web/20200228224625/https://pdfs.semanticscholar.org/ccc3/cb3422d8b2b02f66515d45710a09df8c56d0.pdf) (PDF) (Thesis). Bibcode:2009PhDT.....94Z (https://ui.adsabs.harvard.edu/abs/2009PhDT.....94Z). S2CID 118227839 (https://api.semanticscholar.org/CorpusID:118227839). Archived from the original (https://pdfs.semanticscholar.org/ccc3/cb3422d8b2b02f66515d45710a09df8c56d0.pdf) (PDF) on 28 February 2020.
112. Lo, Hoi-Kwong (22 October 2005). "Decoy State Quantum Key Distribution" (https://dx.doi.org/10.1142/9789812701633_0013). *Quantum Information Science*. **94** (23). WORLD SCIENTIFIC: 143. arXiv:quant-ph/0411004 (https://arxiv.org/abs/quant-ph/0411004). Bibcode:2005qis..conf..143L (https://ui.adsabs.harvard.edu/abs/2005qis..conf..143L). doi:10.1142/9789812701633_0013 (https://doi.org/10.1142%2F9789812701633_0013). ISBN 978-981-256-460-3. PMID 16090452 (https://pubmed.ncbi.nlm.nih.gov/16090452).

113. Reimer, Michael E.; Cher, Catherine (November 2019). "The quest for a perfect single-photon source" (https://www.nature.com/articles/s41566-019-0544-x). *Nature Photonics*. **13** (11): 734–736. Bibcode:2019NaPho..13..734R (https://ui.adsabs.harvard.edu/abs/2019NaPho..13..734R). doi:10.1038/s41566-019-0544-x (https://doi.org/10.1038%2Fs41566-019-0544-x). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893). S2CID 209939102 (https://api.semanticscholar.org/CorpusID:209939102).
114. Makarov, Vadim; Anisimov, Andrey; Skaar, Johannes (31 July 2008). "Erratum: Effects of detector efficiency mismatch on security of quantum cryptosystems [Phys. Rev. A74, 022313 (2006)]" (https://doi.org/10.1103%2Fphysreva.78.019905). *Physical Review A*. **78** (1): 019905. Bibcode:2008PhRvA..78a9905M (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78a9905M). doi:10.1103/physreva.78.019905 (https://doi.org/10.1103%2Fphysreva.78.019905). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947).
115. "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)" (https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/). National Security Agency. Retrieved 16 July 2022. This article incorporates text from this source, which is in the public domain.
116. Post-Quantum Cryptography: Current state and quantum mitigation, Section 6 "Conclusion" [1] (https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation)
117. Quantum security technologies (https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies)
118. Should Quantum Key Distribution be Used for Secure Communications? (https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/)
119. "Quantum Cryptography" (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Quantenkryptografie/quantenkryptografie.html).
120. Scarani, Valerio; Kurtsiefer, Christian (4 December 2014). "The black paper of quantum cryptography: Real implementation problems" (https://doi.org/10.1016/j.tcs.2014.09.015). *Theoretical Computer Science*. **560**: 27–32. arXiv:0906.4547 (https://arxiv.org/abs/0906.4547). doi:10.1016/j.tcs.2014.09.015 (https://doi.org/10.1016%2Fj.tcs.2014.09.015). S2CID 44504715 (https://api.semanticscholar.org/CorpusID:44504715).
121. Pacher, Christoph; et, al. (January 2016). "Attacks on quantum key distribution protocols that employ non-ITS authentication" (https://doi.org/10.1007/s11128-015-1160-4). *Quantum Information Processing*. **15** (1): 327–362. arXiv:1209.0365 (https://arxiv.org/abs/1209.0365). Bibcode:2016QuIP...15..327P (https://ui.adsabs.harvard.edu/abs/2016QuIP...15..327P). doi:10.1007/s11128-015-1160-4 (https://doi.org/10.1007%2Fs11128-015-1160-4). S2CID 254986932 (https://api.semanticscholar.org/CorpusID:254986932).
122. Mattsson, J. P.; et al. (December 2021). "Quantum-Resistant Cryptography". arXiv:2112.00399 (https://arxiv.org/abs/2112.00399) [cs.CR (https://arxiv.org/archive/cs.CR)].
123. Bloom, Yuval; Fields, Ilai; Maslennikov, Alona; Rozenman, Georgi Gary (2022). "Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation" (https://doi.org/10.3390%2Fphysics4010009). *Physics*. **4** (1): 104–123. Bibcode:2022Physi...4..104B (https://ui.adsabs.harvard.edu/abs/2022Physi...4..104B). doi:10.3390/physics4010009 (https://doi.org/10.3390%2Fphysics4010009).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_cryptography&oldid=1245298957"

WIKIPEDIA
The Free Encyclopedia

Post-quantum cryptography

Post-quantum cryptography (**PQC**), sometimes referred to as **quantum-proof**, **quantum-safe**, or **quantum-resistant**, is the development of cryptographic algorithms (usually public-key algorithms) that are currently thought to be secure against a cryptanalytic attack by a quantum computer. Most widely-used public-key algorithms rely on the difficulty of one of three mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem. All of these problems could be easily solved on a sufficiently powerful quantum computer running Shor's algorithm[1][2] or even faster and less demanding (in terms of the number of qubits required) alternatives.[3]

While, as of 2023, quantum computers lack the processing power to break widely used cryptographic algorithms,[4] cryptographers are designing new algorithms to prepare for **Y2Q** or **Q-Day**, the day when current algorithms will be vulnerable to quantum computing attacks. Their work has gained attention from academics and industry through the PQCrypto conference series hosted since 2006, several workshops on Quantum Safe Cryptography hosted by the European Telecommunications Standards Institute (ETSI), and the Institute for Quantum Computing.[5][6][7] The rumoured existence of widespread harvest now, decrypt later programs has also been seen as a motivation for the early introduction of post-quantum algorithms, as data recorded now may still remain sensitive many years into the future.[8][9][10]

In contrast to the threat quantum computing poses to current public-key algorithms, most current symmetric cryptographic algorithms and hash functions are considered to be relatively secure against attacks by quantum computers.[2][11] While the quantum Grover's algorithm does speed up attacks against symmetric ciphers, doubling the key size can effectively block these attacks.[12] Thus post-quantum symmetric cryptography does not need to differ significantly from current symmetric cryptography.

On August 13, 2024, the U.S. National Institute of Standards and Technology (NIST) released final versions of its first three Post Quantum Crypto Standards.[13]

Algorithms

Post-quantum cryptography research is mostly focused on six different approaches:[2][6]

Lattice-based cryptography

This approach includes cryptographic systems such as learning with errors, ring learning with errors (ring-LWE),[14][15][16] the ring learning with errors key exchange and the ring learning with errors signature, the older NTRU or GGH encryption schemes, and the newer NTRU signature and BLISS signatures.[17] Some of these schemes like NTRU encryption have been studied for many years without anyone finding a feasible attack. Others like the ring-LWE algorithms have proofs that their security reduces to a worst-case problem.[18] The Post Quantum Cryptography Study Group sponsored by the

European Commission suggested that the Stehle–Steinfeld variant of NTRU be studied for standardization rather than the NTRU algorithm.[19][20] At that time, NTRU was still patented. Studies have indicated that NTRU may have more secure properties than other lattice based algorithms.[21]

Multivariate cryptography

This includes cryptographic systems such as the Rainbow (Unbalanced Oil and Vinegar) scheme which is based on the difficulty of solving systems of multivariate equations. Various attempts to build secure multivariate equation encryption schemes have failed. However, multivariate signature schemes like Rainbow could provide the basis for a quantum secure digital signature.[22] The Rainbow Signature Scheme is patented.

Hash-based cryptography

This includes cryptographic systems such as Lamport signatures, the Merkle signature scheme, the XMSS,[23] the SPHINCS,[24] and the WOTS schemes. Hash based digital signatures were invented in the late 1970s by Ralph Merkle and have been studied ever since as an interesting alternative to number-theoretic digital signatures like RSA and DSA. Their primary drawback is that for any hash-based public key, there is a limit on the number of signatures that can be signed using the corresponding set of private keys. This fact reduced interest in these signatures until interest was revived due to the desire for cryptography that was resistant to attack by quantum computers. There appear to be no patents on the Merkle signature scheme and there exist many non-patented hash functions that could be used with these schemes. The stateful hash-based signature scheme XMSS developed by a team of researchers under the direction of Johannes Buchmann is described in RFC 8391.[25]

Note that all the above schemes are one-time or bounded-time signatures, Moni Naor and Moti Yung invented UOWHF hashing in 1989 and designed a signature based on hashing (the Naor-Yung scheme)[26] which can be unlimited-time in use (the first such signature that does not require trapdoor properties).

Code-based cryptography

This includes cryptographic systems which rely on error-correcting codes, such as the McEliece and Niederreiter encryption algorithms and the related Courtois, Finiasz and Sendrier Signature scheme. The original McEliece signature using random Goppa codes has withstood scrutiny for over 40 years. However, many variants of the McEliece scheme, which seek to introduce more structure into the code used in order to reduce the size of the keys, have been shown to be insecure.[27] The Post Quantum Cryptography Study Group sponsored by the European Commission has recommended the McEliece public key encryption system as a candidate for long term protection against attacks by quantum computers.[19]

Isogeny-based cryptography

These cryptographic systems rely on the properties of isogeny graphs of elliptic curves (and higher-dimensional abelian varieties) over finite fields, in particular supersingular isogeny graphs, to create cryptographic systems. Among the more well-known representatives of this field are the Diffie–Hellman-like key exchange *CSIDH*, which can serve as a straightforward quantum-resistant replacement for the

Diffie-Hellman and elliptic curve Diffie–Hellman key-exchange methods that are in widespread use today,[28] and the signature scheme *SQISign* which is based on the categorical equivalence between supersingular elliptic curves and maximal orders in particular types of quaternion algebras.[29] Another widely noticed construction, *SIDH/SIKE*, was spectacularly broken in 2022.[30] The attack is however specific to the SIDH/SIKE family of schemes and does not generalize to other isogeny-based constructions.[31]

Symmetric key quantum resistance

Provided one uses sufficiently large key sizes, the symmetric key cryptographic systems like AES and SNOW 3G are already resistant to attack by a quantum computer.[32] Further, key management systems and protocols that use symmetric key cryptography instead of public key cryptography like Kerberos and the 3GPP Mobile Network Authentication Structure are also inherently secure against attack by a quantum computer. Given its widespread deployment in the world already, some researchers recommend expanded use of Kerberos-like symmetric key management as an efficient way to get post quantum cryptography today.[33]

Security reductions

In cryptography research, it is desirable to prove the equivalence of a cryptographic algorithm and a known hard mathematical problem. These proofs are often called "security reductions", and are used to demonstrate the difficulty of cracking the encryption algorithm. In other words, the security of a given cryptographic algorithm is reduced to the security of a known hard problem. Researchers are actively looking for security reductions in the prospects for post quantum cryptography. Current results are given here:

Lattice-based cryptography – Ring-LWE Signature

In some versions of Ring-LWE there is a security reduction to the shortest-vector problem (SVP) in a lattice as a lower bound on the security. The SVP is known to be NP-hard.[34] Specific ring-LWE systems that have provable security reductions include a variant of Lyubashevsky's ring-LWE signatures defined in a paper by Güneysu, Lyubashevsky, and Pöppelmann.[15] The GLYPH signature scheme is a variant of the Güneysu, Lyubashevsky, and Pöppelmann (GLP) signature which takes into account research results that have come after the publication of the GLP signature in 2012. Another Ring-LWE signature is Ring-TESLA.[35] There also exists a "derandomized variant" of LWE, called Learning with Rounding (LWR), which yields "improved speedup (by eliminating sampling small errors from a Gaussian-like distribution with deterministic errors) and bandwidth".[36] While LWE utilizes the addition of a small error to conceal the lower bits, LWR utilizes rounding for the same purpose.

Lattice-based cryptography – NTRU, BLISS

The security of the NTRU encryption scheme and the BLISS[17] signature is believed to be related to, but not provably reducible to, the closest vector problem (CVP) in a lattice. The CVP is known to be NP-hard. The Post Quantum Cryptography Study Group sponsored by the European Commission suggested that the Stehle–Steinfeld variant of NTRU, which *does* have a security reduction be studied for long term use instead of the original NTRU algorithm.[19]

Multivariate cryptography – Unbalanced oil and vinegar

Unbalanced Oil and Vinegar signature schemes are asymmetric cryptographic primitives based on multivariate polynomials over a finite field $\mathbb{F}$. Bulygin, Petzoldt and Buchmann have shown a reduction of generic multivariate quadratic UOV systems to the NP-Hard multivariate quadratic equation solving problem.[37]

Hash-based cryptography – Merkle signature scheme

In 2005, Luis Garcia proved that there was a security reduction of Merkle Hash Tree signatures to the security of the underlying hash function. Garcia showed in his paper that if computationally one-way hash functions exist then the Merkle Hash Tree signature is provably secure.[38]

Therefore, if one used a hash function with a provable reduction of security to a known hard problem one would have a provable security reduction of the Merkle tree signature to that known hard problem.[39]

The Post Quantum Cryptography Study Group sponsored by the European Commission has recommended use of Merkle signature scheme for long term security protection against quantum computers.[19]

Code-based cryptography – McEliece

The McEliece Encryption System has a security reduction to the syndrome decoding problem (SDP). The SDP is known to be NP-hard.[40] The Post Quantum Cryptography Study Group sponsored by the European Commission has recommended the use of this cryptography for long term protection against attack by a quantum computer.[19]

Code-based cryptography – RLCE

In 2016, Wang proposed a random linear code encryption scheme RLCE[41] which is based on McEliece schemes. RLCE scheme can be constructed using any linear code such as Reed-Solomon code by inserting random columns in the underlying linear code generator matrix.

Supersingular elliptic curve isogeny cryptography

Security is related to the problem of constructing an isogeny between two supersingular curves with the same number of points. The most recent investigation of the difficulty of this problem is by Delfs and Galbraith indicates that this problem is as hard as the inventors of the key exchange suggest that it is.[42] There is no security reduction to a known NP-hard problem.

Comparison

One common characteristic of many post-quantum cryptography algorithms is that they require larger key sizes than commonly used "pre-quantum" public key algorithms. There are often tradeoffs to be made in key size, computational efficiency and ciphertext or signature size. The table lists some values for different schemes at a 128-bit post-quantum security level.

Algorithm	Type	Public key	Private key	Signature
NTRU Encrypt[43]	Lattice	766.25 B	842.875 B	
Streamlined NTRU Prime	Lattice	154 B		
Rainbow[44]	Multivariate	124 kB	95 kB	
SPHINCS[24]	Hash Signature	1 kB	1 kB	41 kB
SPHINCS+[45]	Hash Signature	32 B	64 B	8 kB
BLISS-II	Lattice	7 kB	2 kB	5 kB
GLP-Variant GLYPH Signature[15][46]	Ring-LWE	2 kB	0.4 kB	1.8 kB
NewHope[47]	Ring-LWE	2 kB	2 kB	
Goppa-based McEliece[19]	Code-based	1 MB	11.5 kB	
Random Linear Code based encryption[48]	RLCE	115 kB	3 kB	
Quasi-cyclic MDPC-based McEliece[49]	Code-based	1,232 B	2,464 B	
SIDH[50]	Isogeny	564 B	48 B	
SIDH (compressed keys)[51]	Isogeny	330 B	48 B	
3072-bit Discrete Log	**not PQC**	384 B	32 B	96 B
256-bit Elliptic Curve	**not PQC**	32 B	32 B	65 B

A practical consideration on a choice among post-quantum cryptographic algorithms is the effort required to send public keys over the internet. From this point of view, the Ring-LWE, NTRU, and SIDH algorithms provide key sizes conveniently under 1 kB, hash-signature public keys come in under 5 kB, and MDPC-based McEliece takes about 1 kB. On the other hand, Rainbow schemes require about 125 kB and Goppa-based McEliece requires a nearly 1 MB key.

Lattice-based cryptography – LWE key exchange and Ring-LWE key exchange

The fundamental idea of using LWE and Ring LWE for key exchange was proposed and filed at the University of Cincinnati in 2011 by Jintai Ding. The basic idea comes from the associativity of matrix multiplications, and the errors are used to provide the security. The paper[52] appeared in 2012 after a

provisional patent application was filed in 2012.

In 2014, Peikert[53] presented a key transport scheme following the same basic idea of Ding's, where the new idea of sending additional 1 bit signal for rounding in Ding's construction is also utilized. For somewhat greater than 128 bits of security, Singh presents a set of parameters which have 6956-bit public keys for the Peikert's scheme.[54] The corresponding private key would be roughly 14,000 bits.

In 2015, an authenticated key exchange with provable forward security following the same basic idea of Ding's was presented at Eurocrypt 2015,[55] which is an extension of the HMQV[56] construction in Crypto2005. The parameters for different security levels from 80 bits to 350 bits, along with the corresponding key sizes are provided in the paper.[55]

Lattice-based cryptography – NTRU encryption

For 128 bits of security in NTRU, Hirschhorn, Hoffstein, Howgrave-Graham and Whyte, recommend using a public key represented as a degree 613 polynomial with coefficients $\mod \left(2^{10}\right)$ This results in a public key of 6130 bits. The corresponding private key would be 6743 bits.[43]

Multivariate cryptography – Rainbow signature

For 128 bits of security and the smallest signature size in a Rainbow multivariate quadratic equation signature scheme, Petzoldt, Bulygin and Buchmann, recommend using equations in $\mathbb{F}_{31}$ with a public key size of just over 991,000 bits, a private key of just over 740,000 bits and digital signatures which are 424 bits in length.[44]

Hash-based cryptography – Merkle signature scheme

In order to get 128 bits of security for hash based signatures to sign 1 million messages using the fractal Merkle tree method of Naor Shenhav and Wool the public and private key sizes are roughly 36,000 bits in length.[57]

Code-based cryptography – McEliece

For 128 bits of security in a McEliece scheme, The European Commissions Post Quantum Cryptography Study group recommends using a binary Goppa code of length at least $n = 6960$ and dimension at least $k = 5413$, and capable of correcting $t = 119$ errors. With these parameters the public key for the McEliece system will be a systematic generator matrix whose non-identity part takes $k \times (n - k) = 8373911$ bits. The corresponding private key, which consists of the code support with $n = 6960$ elements from $\mathrm{GF}(2^{13})$ and a generator polynomial of with $t = 119$ coefficients from $\mathrm{GF}(2^{13})$, will be 92,027 bits in length[19]

The group is also investigating the use of Quasi-cyclic MDPC codes of length at least $n = 2^{16} + 6 = 65542$ and dimension at least $k = 2^{15} + 3 = 32771$, and capable of correcting $t = 264$ errors. With these parameters the public key for the McEliece system will be the first row of a systematic generator matrix whose non-identity part takes $k = 32771$ bits. The private key, a quasi-cyclic parity-check matrix with $d = 274$ nonzero entries on a column (or twice as much on a row), takes no more than $d \times 16 = 4384$ bits when represented as the coordinates of the nonzero entries on the first row.

Barreto et al. recommend using a binary Goppa code of length at least $n = 3307$ and dimension at least $k = 2515$, and capable of correcting $t = 66$ errors. With these parameters the public key for the McEliece system will be a systematic generator matrix whose non-identity part takes $k \times (n - k) = 1991880$ bits.[58] The corresponding private key, which consists of the code support with $n = 3307$ elements from $\mathrm{GF}(2^{12})$ and a generator polynomial of with $t = 66$ coefficients from $\mathrm{GF}(2^{12})$, will be 40,476 bits in length.

Supersingular elliptic curve isogeny cryptography

For 128 bits of security in the supersingular isogeny Diffie-Hellman (SIDH) method, De Feo, Jao and Plut recommend using a supersingular curve modulo a 768-bit prime. If one uses elliptic curve point compression the public key will need to be no more than 8x768 or 6144 bits in length.[59] A March 2016 paper by authors Azarderakhsh, Jao, Kalach, Koziel, and Leonardi showed how to cut the number of bits transmitted in half, which was further improved by authors Costello, Jao, Longa, Naehrig, Renes and Urbanik resulting in a compressed-key version of the SIDH protocol with public keys only 2640 bits in size.[51] This makes the number of bits transmitted roughly equivalent to the non-quantum secure RSA and Diffie-Hellman at the same classical security level.[60]

Symmetric–key-based cryptography

As a general rule, for 128 bits of security in a symmetric-key-based system, one can safely use key sizes of 256 bits. The best quantum attack against arbitrary symmetric-key systems is an application of Grover's algorithm, which requires work proportional to the square root of the size of the key space. To transmit an encrypted key to a device that possesses the symmetric key necessary to decrypt that key requires roughly 256 bits as well. It is clear that symmetric-key systems offer the smallest key sizes for post-quantum cryptography.

Forward secrecy

A public-key system demonstrates a property referred to as perfect forward secrecy when it generates random public keys per session for the purposes of key agreement. This means that the compromise of one message cannot lead to the compromise of others, and also that there is not a single secret value which can lead to the compromise of multiple messages. Security experts recommend using cryptographic algorithms that support forward secrecy over those that do not.[61] The reason for this is that forward secrecy can protect against the compromise of long term private keys associated with public/private key pairs. This is viewed as a means of preventing mass surveillance by intelligence agencies.

Both the Ring-LWE key exchange and supersingular isogeny Diffie-Hellman (SIDH) key exchange can support forward secrecy in one exchange with the other party. Both the Ring-LWE and SIDH can also be used without forward secrecy by creating a variant of the classic ElGamal encryption variant of Diffie-Hellman.

The other algorithms in this article, such as NTRU, do not support forward secrecy as is.

Any authenticated public key encryption system can be used to build a key exchange with forward secrecy.[62]

Open Quantum Safe project

The **Open Quantum Safe** (**OQS**) project was started in late 2016 and has the goal of developing and prototyping quantum-resistant cryptography.[63][64] It aims to integrate current post-quantum schemes in one library: **liboqs**.[65] liboqs is an open source C library for quantum-resistant cryptographic algorithms. It initially focuses on key exchange algorithms but by now includes several signature schemes. It provides a common API suitable for post-quantum key exchange algorithms, and will collect together various implementations. liboqs will also include a test harness and benchmarking routines to compare performance of post-quantum implementations. Furthermore, OQS also provides integration of liboqs into OpenSSL.[66]

As of March 2023, the following key exchange algorithms are supported:[63]

Algorithm	Type
CRYSTALS-Kyber	Module Learning With Error
Classic McEliece	goppa codes
BIKE[67]	codes
HQC[68][69]	codes
Frodo[70][71]	Learning with errors
NTRU[72]	Lattice-based cryptography
CRYSTALS-Dilithium[73][74]	Module Short Integer Solution
Falcon	Short Integer Solution
SPHINCS+	hash based

Older supported versions that have been removed because of the progression of the NIST Post-Quantum Cryptography Standardization Project are:

Algorithm	Type
BCNS15[75]	Ring learning with errors key exchange
NewHope[76][47]	Ring learning with errors key exchange
SIDH[77][78]	Supersingular isogeny key exchange
McBits[79]	Error-correcting codes

Implementation

One of the main challenges in post-quantum cryptography is considered to be the implementation of potentially quantum safe algorithms into existing systems. There are tests done, for example by Microsoft Research implementing PICNIC in a PKI using Hardware security modules.[80] Test implementations for

Google's NewHope algorithm have also been done by HSM vendors. In August 2023, Google released a FIDO2 security key implementation of an ECC/Dilithium hybrid signature schema which was done in partnership with ETH Zürich.[81]

On February 21, 2024, Apple announced that they were going to upgrade their iMessage protocol with a new PQC protocol called "PQ3", which will utilize ongoing keying.[82][83][84] Apple stated that, although quantum computers don't exist yet, they wanted to mitigate risks from future quantum computers as well as so-called "Harvest now, decrypt later" attack scenarios. Apple stated that they believe their PQ3 implementation provides protections that "surpass those in all other widely deployed messaging apps, because it utilizes ongoing keying. Apple intends to fully replace the existing iMessage protocol within all supported conversations with PQ3 by the end of 2024. Apple also defined a scale to make it easier to compare the security properties of messaging apps, with a scale represented by levels ranging from 0 to 3.[82]

Other notable implementations include:

- bouncycastle[85]
- liboqs[86]

See also

- NIST Post-Quantum Cryptography Standardization
- Quantum cryptography – cryptography based on quantum mechanics
- Crypto-shredding – Deleting encryption keys
- Harvest now, decrypt later

References

1. Shor, Peter W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing*. **26** (5): 1484–1509. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). Bibcode:1995quant.ph..8027S (https://ui.adsabs.harvard.edu/abs/1995quant.ph..8027S). doi:10.1137/S0097539795293172 (https://doi.org/10.1137%2FS0097539795293172). S2CID 2337707 (https://api.semanticscholar.org/CorpusID:2337707).
2. Bernstein, Daniel J. (2009). "Introduction to post-quantum cryptography" (http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf) (PDF). *Post-Quantum Cryptography*.
3. Kramer, Anna (2023). "'Surprising and super cool.' Quantum algorithm offers faster way to hack internet encryption" (https://www.science.org/content/article/surprising-and-supercool-quantum-algorithm-offers-faster-way-hack-internet-encryption). *Science*. **381** (6664): 1270. doi:10.1126/science.adk9443 (https://doi.org/10.1126%2Fscience.adk9443). PMID 37733849 (https://pubmed.ncbi.nlm.nih.gov/37733849). S2CID 262084525 (https://api.semanticscholar.org/CorpusID:262084525).
4. "New qubit control bodes well for future of quantum computing" (http://phys.org/news/2013-01-qubit-bodes-future-quantum.html). *phys.org*.
5. "Cryptographers Take On Quantum Computers" (https://spectrum.ieee.org/cryptographers-take-on-quantum-computers). *IEEE Spectrum*. 2009-01-01.

6. "Q&A With Post-Quantum Computing Cryptography Researcher Jintai Ding" (https://spectrum.ieee.org/qa-with-postquantum-computing-cryptography-researcher-jintai-ding). *IEEE Spectrum*. 2008-11-01.
7. "ETSI Quantum Safe Cryptography Workshop" (https://web.archive.org/web/20160817044813/http://www.etsi.org/news-events/events/770-etsi-crypto-workshop-2014?highlight=YTozOntpOjA7czo3OiJxdWFudHVtIjtpOjE7czo0OiJzYWZlIjtpOjI7czoxMjoicXVhbnR1bSBzYWZlIjt9). *ETSI Quantum Safe Cryptography Workshop*. ETSI. October 2014. Archived from the original (http://www.etsi.org/news-events/events/770-etsi-crypto-workshop-2014?highlight=YTozOntpOjA7czo3OiJxdWFudHVtIjtpOjE7czo0OiJzYWZlIjtpOjI7czoxMjoicXVhbnR1bSBzYWZlIjt9) on 17 August 2016. Retrieved 24 February 2015.
8. Gasser, Linus (2023), Mulder, Valentin; Mermoud, Alain; Lenders, Vincent; Tellenbach, Bernhard (eds.), "Post-quantum Cryptography", *Trends in Data Protection and Encryption Technologies*, Cham: Springer Nature Switzerland, pp. 47–52, doi:10.1007/978-3-031-33386-6_10 (https://doi.org/10.1007%2F978-3-031-33386-6_10), ISBN 978-3-031-33386-6
9. Townsend, Kevin (2022-02-16). "Solving the Quantum Decryption 'Harvest Now, Decrypt Later' Problem" (https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/). *SecurityWeek*. Retrieved 2023-04-09.
10. "Quantum-Safe Secure Communications" (https://uknqt.ukri.org/wp-content/uploads/2021/10/Quantum-Safe-Secure-Communications.pdf) (PDF). *UK National Quantum Technologies Programme*. October 2021. Retrieved 2023-04-09.
11. Daniel J. Bernstein (2009-05-17). "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?" (http://cr.yp.to/hash/collisioncost-20090823.pdf) (PDF).
12. Daniel J. Bernstein (2010-03-03). "Grover vs. McEliece" (http://cr.yp.to/codes/grovercode-20100303.pdf) (PDF).
13. NIST Releases First 3 Finalized Post-Quantum Encryption Standards (https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards), NIST, August 13, 2024
14. Peikert, Chris (2014). "Lattice Cryptography for the Internet" (https://web.archive.org/web/20140512214902/http://eprint.iacr.org/2014/070.pdf) (PDF). IACR. Archived from the original on 12 May 2014. Retrieved 10 May 2014.
15. Güneysu, Tim; Lyubashevsky, Vadim; Pöppelmann, Thomas (2012). "Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems" (http://emsec.rub.de/media/sh/veroeffentlichungen/2014/06/12/lattice_signature.pdf) (PDF). INRIA. Retrieved 12 May 2014.
16. Zhang, jiang (2014). "Authenticated Key Exchange from Ideal Lattices" (https://web.archive.org/web/20140907212538/http://eprint.iacr.org/2014/589.pdf) (PDF). *iacr.org*. IACR. Archived from the original on 7 September 2014. Retrieved 7 September 2014.
17. Ducas, Léo; Durmus, Alain; Lepoint, Tancrède; Lyubashevsky, Vadim (2013). "Lattice Signatures and Bimodal Gaussians" (http://eprint.iacr.org/2013/383). *Cryptology ePrint Archive*. Retrieved 2015-04-18.
18. Lyubashevsky, Vadim; Peikert; Regev (2013). "On Ideal Lattices and Learning with Errors Over Rings" (https://web.archive.org/web/20140131051244/http://eprint.iacr.org/2012/230.pdf) (PDF). IACR. Archived from the original on 31 January 2014. Retrieved 14 May 2013.
19. Augot, Daniel (7 September 2015). "Initial recommendations of long-term secure post-quantum systems" (http://pqcrypto.eu.org/docs/initial-recommendations.pdf) (PDF). *PQCRYPTO*. Retrieved 13 September 2015.
20. Stehlé, Damien; Steinfeld, Ron (2013-01-01). "Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices" (http://eprint.iacr.org/2013/004). *Cryptology ePrint Archive*.

21. Easttom, Chuck (2019-02-01). "An Analysis of Leading Lattice-Based Asymmetric Cryptographic Primitives". *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. pp. 0811–0818. doi:10.1109/CCWC.2019.8666459 (https://doi.org/10.1109%2FCCWC.2019.8666459). ISBN 978-1-7281-0554-3. S2CID 77376310 (https://api.semanticscholar.org/CorpusID:77376310).
22. Ding, Jintai; Schmidt (7 June 2005). "Rainbow, a New Multivariable Polynomial Signature Scheme". In Ioannidis, John (ed.). *Applied Cryptography and Network Security*. Lecture Notes in Computer Science. Vol. 3531. pp. 64–175. doi:10.1007/11496137_12 (https://doi.org/10.1007%2F11496137_12). ISBN 978-3-540-26223-7. S2CID 6571152 (https://api.semanticscholar.org/CorpusID:6571152).
23. Buchmann, Johannes; Dahmen, Erik; Hülsing, Andreas (2011). "XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions". *Post-Quantum Cryptography. PQCrypto 2011*. Lecture Notes in Computer Science. Vol. 7071. pp. 117–129. CiteSeerX 10.1.1.400.6086 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.400.6086). doi:10.1007/978-3-642-25405-5_8 (https://doi.org/10.1007%2F978-3-642-25405-5_8). ISBN 978-3-642-25404-8. ISSN 0302-9743 (https://search.worldcat.org/issn/0302-9743).
24. Bernstein, Daniel J.; Hopwood, Daira; Hülsing, Andreas; Lange, Tanja; Niederhagen, Ruben; Papachristodoulou, Louiza; Schneider, Michael; Schwabe, Peter; Wilcox-O'Hearn, Zooko (2015). "SPHINCS: Practical Stateless Hash-Based Signatures". In Oswald, Elisabeth; Fischlin, Marc (eds.). *Advances in Cryptology -- EUROCRYPT 2015*. Lecture Notes in Computer Science. Vol. 9056. Springer Berlin Heidelberg. pp. 368–397. CiteSeerX 10.1.1.690.6403 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.690.6403). doi:10.1007/978-3-662-46800-5_15 (https://doi.org/10.1007%2F978-3-662-46800-5_15). ISBN 9783662467992.
25. Huelsing, A.; Butin, D.; Gazdag, S.; Rijneveld, J.; Mohaisen, A. (2018). "RFC 8391 – XMSS: eXtended Merkle Signature Scheme" (https://tools.ietf.org/html/rfc8391). *tools.ietf.org*. doi:10.17487/RFC8391 (https://doi.org/10.17487%2FRFC8391).
26. Naor, Moni; Yung, Moti (1989), *Universal One-Way Hash Functions and their Cryptographic Applications .STOC*, pp. 33–43
27. Overbeck, Raphael; Sendrier (2009). "Code-based cryptography". In Bernstein, Daniel (ed.). *Post-Quantum Cryptography*. pp. 95–145. doi:10.1007/978-3-540-88702-7_4 (https://doi.org/10.1007%2F978-3-540-88702-7_4). ISBN 978-3-540-88701-0.
28. Castryck, Wouter; Lange, Tanja; Martindale, Chloe; Panny, Lorenz; Renes, Joost (2018). "CSIDH: An Efficient Post-Quantum Commutative Group Action" (https://hdl.handle.net/handle/1854/LU-8619033). In Peyrin, Thomas; Galbraith, Steven (eds.). *Advances in Cryptology – ASIACRYPT 2018*. Lecture Notes in Computer Science. Vol. 11274. Cham: Springer International Publishing. pp. 395–427. doi:10.1007/978-3-030-03332-3_15 (https://doi.org/10.1007%2F978-3-030-03332-3_15). hdl:1854/LU-8619033 (https://hdl.handle.net/1854%2FLU-8619033). ISBN 978-3-030-03332-3. S2CID 44165584 (https://api.semanticscholar.org/CorpusID:44165584).
29. De Feo, Luca; Kohel, David; Leroux, Antonin; Petit, Christophe; Wesolowski, Benjamin (2020). "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies" (https://hal.archives-ouvertes.fr/hal-03038004/file/2020-1240.pdf) (PDF). In Moriai, Shiho; Wang, Huaxiong (eds.). *Advances in Cryptology – ASIACRYPT 2020*. Lecture Notes in Computer Science. Vol. 12491. Cham: Springer International Publishing. pp. 64–93. doi:10.1007/978-3-030-64837-4_3 (https://doi.org/10.1007%2F978-3-030-64837-4_3). ISBN 978-3-030-64837-4. S2CID 222265162 (https://api.semanticscholar.org/CorpusID:222265162).

30. Castryck, Wouter; Decru, Thomas (2023), Hazay, Carmit; Stam, Martijn (eds.), "An Efficient Key Recovery Attack on SIDH" (https://link.springer.com/10.1007/978-3-031-30589-4_15), *Advances in Cryptology – EUROCRYPT 2023*, vol. 14008, Cham: Springer Nature Switzerland, pp. 423–447, doi:10.1007/978-3-031-30589-4_15 (https://doi.org/10.1007%2F978-3-031-30589-4_15), ISBN 978-3-031-30588-7, S2CID 258240788 (https://api.semanticscholar.org/CorpusID:258240788), retrieved 2023-06-21
31. "Is SIKE broken yet?" (https://issikebrokenyet.github.io/). Retrieved 2023-06-23.
32. Perlner, Ray; Cooper (2009). *Quantum Resistant Public Key Cryptography: A Survey* (https://www.nist.gov/manuscript-publication-search.cfm?pub_id=901595). 8th Symposium on Identity and Trust on the Internet (IDtrust 2009). NIST. Retrieved 23 Apr 2015.
33. Campagna, Matt; Hardjono; Pintsov; Romansky; Yu (2013). "Kerberos Revisited Quantum-Safe Authentication" (http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/S03_INDUSTRY_SESSION/PITNEYBOWES_PINTSOV.pdf) (PDF). ETSI.
34. Lyubashevsky, Vadim; Peikert; Regev (25 June 2013). "On Ideal Lattices and Learning with Errors Over Rings" (https://web.eecs.umich.edu/~cpeikert/pubs/ideal-lwe.pdf) (PDF). Springer. Retrieved 19 June 2014.
35. Akleylek, Sedat; Bindel, Nina; Buchmann, Johannes; Krämer, Juliane; Marson, Giorgia Azzurra (2016). "An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation" (https://eprint.iacr.org/2016/030). *Cryptology ePrint Archive*.
36. Nejatollahi, Hamid; Dutt, Nikil; Ray, Sandip; Regazzoni, Francesco; Banerjee, Indranil; Cammarota, Rosario (2019-02-27). "Post-Quantum Lattice-Based Cryptography Implementations: A Survey" (https://dl.acm.org/doi/10.1145/3292548). *ACM Computing Surveys*. **51** (6): 1–41. doi:10.1145/3292548 (https://doi.org/10.1145%2F3292548). ISSN 0360-0300 (https://search.worldcat.org/issn/0360-0300). S2CID 59337649 (https://api.semanticscholar.org/CorpusID:59337649).
37. Bulygin, Stanislav; Petzoldt; Buchmann (2010). "Towards Provable Security of the Unbalanced Oil and Vinegar Signature Scheme under Direct Attacks". *Progress in Cryptology – INDOCRYPT 2010*. Lecture Notes in Computer Science. Vol. 6498. pp. 17–32. CiteSeerX 10.1.1.294.3105 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.294.3105). doi:10.1007/978-3-642-17401-8_3 (https://doi.org/10.1007%2F978-3-642-17401-8_3). ISBN 978-3-642-17400-1.
38. Pereira, Geovandro; Puodzius, Cassius; Barreto, Paulo (2016). "Shorter hash-based signatures". *Journal of Systems and Software*. **116**: 95–100. doi:10.1016/j.jss.2015.07.007 (https://doi.org/10.1016%2Fj.jss.2015.07.007).
39. Garcia, Luis. "On the security and the efficiency of the Merkle signature scheme" (http://eprint.iacr.org/2005/192.pdf) (PDF). *Cryptology ePrint Archive*. IACR. Retrieved 19 June 2013.
40. Blaum, Mario; Farrell; Tilborg (31 May 2002). *Information, Coding and Mathematics*. Springer. ISBN 978-1-4757-3585-7.
41. Wang, Yongge (2016). "Quantum resistant random linear code based public key encryption scheme RLCE". *Proceedings of Information Theory (ISIT)*. IEEE ISIT: 2519–2523. arXiv:1512.08454 (https://arxiv.org/abs/1512.08454). Bibcode:2015arXiv151208454W (https://ui.adsabs.harvard.edu/abs/2015arXiv151208454W).
42. Delfs, Christina; Galbraith (2013). "Computing isogenies between supersingular elliptic curves over F_p". arXiv:1310.7789 (https://arxiv.org/abs/1310.7789) [math.NT (https://arxiv.org/archive/math.NT)].
43. Hirschborrn, P; Hoffstein; Howgrave-Graham; Whyte. "Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches" (https://web.archive.org/web/20130130160705/https://securityinnovation.com/uploads/Crypto/params.pdf) (PDF). NTRU. Archived from the original (https://www.securityinnovation.com/uploads/Crypto/params.pdf) (PDF) on 30 January 2013. Retrieved 12 May 2014.

44. Petzoldt, Albrecht; Bulygin; Buchmann (2010). "Selecting Parameters for the Rainbow Signature Scheme – Extended Version -" (https://web.archive.org/web/20160304001111/http://eprint.iacr.org/2010/437.pdf) (PDF). Archived from the original on 4 March 2016. Retrieved 12 May 2014.
45. "SPHINCS+: Submission to the NIST post-quantum project" (https://sphincs.org/data/sphincs+-specification.pdf) (PDF).
46. Chopra, Arjun (2017). "GLYPH: A New Insantiation of the GLP Digital Signature Scheme" (https://eprint.iacr.org/2017/766). *Cryptology ePrint Archive*.
47. Alkim, Erdem; Ducas, Léo; Pöppelmann, Thomas; Schwabe, Peter (2015). "Post-quantum key exchange – a new hope" (http://eprint.iacr.org/2015/1092) (PDF). Cryptology ePrint Archive, Report 2015/1092. Retrieved 1 September 2017.
48. Wang, Yongge (2017). "Revised Quantum Resistant Public Key Encryption Scheme RLCE and IND-CCA2 Security for McEliece Schemes" (https://eprint.iacr.org/2017/206). *Cryptology ePrint Archive*.
49. Misoczki, R.; Tillich, J. P.; Sendrier, N.; Barreto, P. S. L. M. (2013). "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes". *2013 IEEE International Symposium on Information Theory*. pp. 2069–2073. CiteSeerX 10.1.1.259.9109 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.259.9109). doi:10.1109/ISIT.2013.6620590 (https://doi.org/10.1109%2FISIT.2013.6620590). ISBN 978-1-4799-0446-4. S2CID 9485532 (https://api.semanticscholar.org/CorpusID:9485532).
50. Costello, Craig; Longa, Patrick; Naehrig, Michael (2016). "Efficient Algorithms for Supersingular Isogeny Diffie-Hellman" (http://eprint.iacr.org/2016/413.pdf) (PDF). *Advances in Cryptology – CRYPTO 2016*. Lecture Notes in Computer Science. Vol. 9814. pp. 572–601. doi:10.1007/978-3-662-53018-4_21 (https://doi.org/10.1007%2F978-3-662-53018-4_21). ISBN 978-3-662-53017-7.
51. Costello, Craig; Jao; Longa; Naehrig; Renes; Urbanik. "Efficient Compression of SIDH public keys" (https://eprint.iacr.org/2016/963). Retrieved 8 October 2016.
52. Ding, Jintai; Xie, Xiang; Lin, Xiaodong (2012-01-01). "A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem" (http://eprint.iacr.org/2012/688). *Cryptology ePrint Archive*.
53. Peikert, Chris (2014-01-01). "Lattice Cryptography for the Internet" (http://eprint.iacr.org/2014/070). *Cryptology ePrint Archive*.
54. Singh, Vikram (2015). "A Practical Key Exchange for the Internet using Lattice Cryptography" (http://eprint.iacr.org/2015/138). *Cryptology ePrint Archive*. Retrieved 2015-04-18.
55. Zhang, Jiang; Zhang, Zhenfeng; Ding, Jintai; Snook, Michael; Dagdelen, Özgür (2015-04-26). "Authenticated Key Exchange from Ideal Lattices". In Oswald, Elisabeth; Fischlin, Marc (eds.). *Advances in Cryptology – EUROCRYPT 2015*. Lecture Notes in Computer Science. Vol. 9057. Springer Berlin Heidelberg. pp. 719–751. CiteSeerX 10.1.1.649.1864 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.649.1864). doi:10.1007/978-3-662-46803-6_24 (https://doi.org/10.1007%2F978-3-662-46803-6_24). ISBN 978-3-662-46802-9.
56. Krawczyk, Hugo (2005-08-14). "HMQV: A High-Performance Secure Diffie-Hellman Protocol". In Shoup, Victor (ed.). *Advances in Cryptology – CRYPTO 2005*. Lecture Notes in Computer Science. Vol. 3621. Springer. pp. 546–566. doi:10.1007/11535218_33 (https://doi.org/10.1007%2F11535218_33). ISBN 978-3-540-28114-6.
57. Naor, Dalit; Shenhav; Wool (2006). "One-Time Signatures Revisited: Practical Fast Signatures Using Fractal Merkle Tree Traversal" (http://www.eng.tau.ac.il/~yash/Naor_Shenhav_Wool.pdf) (PDF). IEEE. Retrieved 13 May 2014.

58. Barreto, Paulo S. L. M.; Biasi, Felipe Piazza; Dahab, Ricardo; López-Hernández, Julio César; Morais, Eduardo M. de; Oliveira, Ana D. Salina de; Pereira, Geovandro C. C. F.; Ricardini, Jefferson E. (2014). Koç, Çetin Kaya (ed.). *A Panorama of Post-quantum Cryptography*. Springer International Publishing. pp. 387–439. doi:10.1007/978-3-319-10683-0_16 (https://doi.org/10.1007%2F978-3-319-10683-0_16). ISBN 978-3-319-10682-3.
59. De Feo, Luca; Jao; Plut (2011). "Towards Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies" (https://web.archive.org/web/20140211082622/http://eprint.iacr.org/2011/506.pdf) (PDF). Archived from the original on 11 February 2014. Retrieved 12 May 2014.
60. "Cryptology ePrint Archive: Report 2016/229" (http://eprint.iacr.org/2016/229). *eprint.iacr.org*. Retrieved 2016-03-02.
61. Ristic, Ivan (2013-06-25). "Deploying Forward Secrecy" (https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy). SSL Labs. Retrieved 14 June 2014.
62. "Does NTRU provide Perfect Forward Secrecy?" (https://crypto.stackexchange.com/a/19115). *crypto.stackexchange.com*.
63. "Open Quantum Safe" (https://openquantumsafe.org/). *openquantumsafe.org*.
64. Stebila, Douglas; Mosca, Michele. "Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project" (http://eprint.iacr.org/2016/1017). *Cryptology ePrint Archive, Report 2016/1017, 2016*. Retrieved 9 April 2017.
65. "liboqs: C library for quantum-resistant cryptographic algorithms" (https://github.com/open-quantum-safe/liboqs). 26 November 2017 – via GitHub.
66. "oqsprovider: Open Quantum Safe provider for OpenSSL (3.x)" (https://github.com/open-quantum-safe/oqs-provider/). 12 August 2024 – via GitHub.
67. "BIKE – Bit Flipping Key Encapsulation" (https://bikesuite.org/). *bikesuite.org*. Retrieved 2023-08-21.
68. "HQC" (https://pqc-hqc.org/). *pqc-hqc.org*. Retrieved 2023-08-21.
69. "Fast and Efficient Hardware Implementation of HQC" (https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/fast-and-efficient-hardware-impl-of-hqc-pqc2022.pdf) (PDF).
70. Bos, Joppe; Costello, Craig; Ducas, Léo; Mironov, Ilya; Naehrig, Michael; Nikolaenko, Valeria; Raghunathan, Ananth; Stebila, Douglas (2016-01-01). "Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE" (http://eprint.iacr.org/2016/659). *Cryptology ePrint Archive*.
71. "FrodoKEM" (https://frodokem.org/). *frodokem.org*. Retrieved 2023-08-21.
72. "NTRUOpenSourceProject/NTRUEncrypt" (https://github.com/NTRUOpenSourceProject/NTRUEncrypt). *GitHub*. Retrieved 2017-04-10.
73. Schwabe, Peter. "Dilithium" (https://pq-crystals.org/dilithium/). *pq-crystals.org*. Retrieved 2023-08-19.
74. "Cryptographic Suite for Algebraic Lattices, Digital Signature: Dilithium" (https://csrc.nist.gov/CSRC/media/Presentations/Crystals-Dilithium/images-media/CRYSTALS-Dilithium-April2018.pdf) (PDF).
75. Stebila, Douglas (26 Mar 2018). "liboqs nist-branch algorithm datasheet: kem_newhopenist" (https://github.com/open-quantum-safe/liboqs/blob/7cc365a363a05cdb233b9d72d0164c123d7b0b65/docs/algorithms/kem_newhopenist.md). *GitHub*. Retrieved 27 September 2018.
76. "Lattice Cryptography Library" (https://www.microsoft.com/en-us/research/project/lattice-cryptography-library/). *Microsoft Research*. 19 Apr 2016. Retrieved 27 September 2018.
77. "SIDH Library – Microsoft Research" (https://www.microsoft.com/en-us/research/project/sidh-library/). *Microsoft Research*. Retrieved 2017-04-10.

78. Feo, Luca De; Jao, David; Plût, Jérôme (2011-01-01). "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies" (https://web.archive.org/web/20140503190338/http://eprint.iacr.org/2011/506). *Cryptology ePrint Archive*. PQCrypto 2011. Archived from the original (https://eprint.iacr.org/2011/506) on 2014-05-03.
79. Bernstein, Daniel J.; Chou, Tung; Schwabe, Peter (2015-01-01). "McBits: fast constant-time code-based cryptography" (https://eprint.iacr.org/2015/610). *Cryptology ePrint Archive*.
80. "Microsoft/Picnic" (https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf) (PDF). *GitHub*. Retrieved 2018-06-27.
81. "Toward Quantum Resilient Security Keys" (https://security.googleblog.com/2023/08/toward-quantum-resilient-security-keys.html). *Google Online Security Blog*. Retrieved 2023-08-19.
82. Apple Security Engineering and Architecture (SEAR) (February 21, 2024). "iMessage with PQ3: The new state of the art in quantum-secure messaging at scale" (https://security.apple.com/blog/imessage-pq3). *Apple Security Research*. Apple Inc. Retrieved 2024-02-22. "With compromise-resilient encryption and extensive defenses against even highly sophisticated quantum attacks, PQ3 is the first messaging protocol to reach what we call Level 3 security — providing protocol protections that surpass those in all other widely deployed messaging apps."
83. Rossignoi, Joe (February 21, 2024). "Apple Announces 'Groundbreaking' New Security Protocol for iMessage" (https://www.macrumors.com/2024/02/21/apple-announces-imessage-security-upgrade/). *MacRumors*. Retrieved 2024-02-22.
84. Potuck, Michael (February 21, 2024). "Apple launching quantum computer protection for iMessage with iOS 17.4, here's what that means" (https://9to5mac.com/2024/02/21/imessage-quantum-security-ios-17-4/). *9to5Mac*. Retrieved 2024-02-22.
85. "Bouncy Castle Betas" (https://downloads.bouncycastle.org/betas).
86. "Open Quantum Safe" (https://openquantumsafe.org/liboqs/).

Further reading

- *Post-Quantum Cryptography* (https://www.springer.com/mathematics/numbers/book/978-3-540-88701-0). Springer. 2008. p. 245. ISBN 978-3-540-88701-0.
- Isogenies in a Quantum World (http://ecc2011.loria.fr/slides/jao.pdf) Archived (https://web.archive.org/web/20140502063037/http://ecc2011.loria.fr/slides/jao.pdf) 2014-05-02 at the Wayback Machine
- On Ideal Lattices and Learning With Errors Over Rings (https://www.di.ens.fr/~pnguyen/LCD/LCD_Vadim.pdf)
- Kerberos Revisited: Quantum-Safe Authentication (http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/S03_INDUSTRY_SESSION/PITNEYBOWES_PINTSOV.pdf)
- The picnic signature scheme (https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf)
- Bernstein, Daniel J.; Lange, Tanja (2017). "Post-quantum cryptography". *Nature*. **549**: 188–194. doi:10.1038/nature23461 (https://doi.org/10.1038%2Fnature23461).
- Campagna, Matt; LaMacchia, Brian; Ott, David (2021). "Post Quantum Cryptography: Readiness Challenges and the Approaching Storm" (https://doi.org/10.48550%2FarXiv.2101.01269). *Computing Community Consortium*. arXiv:2101.01269 (https://arxiv.org/abs/2101.01269). doi:10.48550/arXiv.2101.01269 (https://doi.org/10.48550%2FarXiv.2101.01269).
- Yalamuri, Gagan; Honnavalli, Prasad; Eswaran, Sivaraman (2022). "A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats" (https://doi.org/10.1016%2Fj.procs.2022.12.086). *Procedia Computer Science*. **215**: 834–845. doi:10.1016/j.procs.2022.12.086 (https://doi.org/10.1016%2Fj.procs.2022.12.086).

- Li, Silong; Chen, Yuxiang; Chen, Lin; Liao, Jing; Kuang, Chanchan; Li, Kuanching; Liang, Wei; Xiong, Naixue (2023). "Post-Quantum Security: Opportunities and Challenges" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10648643). *Sensors*. **23** (21): 8744. doi:10.3390/s23218744 (https://doi.org/10.3390%2Fs23218744). PMC 10648643 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10648643).
- Dam, Duc-Thuan; Tran, Thai-Ha; Hoang, Van-Phuc; Pham, Cong-Kha; Hoang, Trong-Thuc (2023). "A Survey of Post-Quantum Cryptography: Start of a New Race" (https://doi.org/10.3390%2Fcryptography7030040). *Cryptography*. **7** (3): 40. doi:10.3390/cryptography7030040 (https://doi.org/10.3390%2Fcryptography7030040).
- Bavdekar, Ritik; Jayant Chopde, Eashan; Agrawal, Ankit; Bhatia, Ashutosh; Tiwari, Kamlesh (2023). "Post Quantum Cryptography: A Review of Techniques, Challenges and Standardizations". *International Conference on Information Networking (ICOIN)*: 146–151. doi:10.1109/ICOIN56518.2023.10048976 (https://doi.org/10.1109%2FICOIN56518.2023.10048976).
- Sood, Neerav (2024). "Cryptography in Post Quantum Computing Era" (https://doi.org/10.2139%2Fssrn.4705470). *SSRN Electronic Journal*. doi:10.2139/ssrn.4705470 (https://doi.org/10.2139%2Fssrn.4705470).
- Rawal, Bharat S.; Curry, Peter J. (2024). "Challenges and opportunities on the horizon of post-quantum cryptography" (https://doi.org/10.1063%2F5.0198344). *APL Quantum*. **1** (2). doi:10.1063/5.0198344 (https://doi.org/10.1063%2F5.0198344).
- Bagirovs, Emils; Provodin, Grigory; Sipola, Tuomo; Hautamäki, Jari (2024). "Applications of Post-quantum Cryptography" (https://doi.org/10.48550%2FarXiv.2406.13258). *European Conference on Cyber Warfare and Security*. **23** (1): 49–57. arXiv:2406.13258 (https://arxiv.org/abs/2406.13258). doi:10.48550/arXiv.2406.13258 (https://doi.org/10.48550%2FarXiv.2406.13258).

External links

- PQCrypto, the post-quantum cryptography conference (http://www.pqcrypto.org/)
- ETSI Quantum Secure Standards Effort (http://www.etsi.org/news-events/news/947-2015-03-news-etsi-launches-quantum-safe-cryptography-specification-group)
- NIST's Post-Quantum crypto Project (http://csrc.nist.gov/groups/ST/post-quantum-crypto/)
- PQCrypto Usage & Deployment (https://ianix.com/pqcrypto/pqcrypto-deployment.html)
- ISO 27001 Certification Cost (https://www.siscertifications.com/iso-27001-certification/)
- ISO 22301:2019 – Security and Resilience in the United States (https://pacificcert.com/iso-22301-2019-security-and-resilience-in-the-united-states/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Post-quantum_cryptography&oldid=1245357128"

WIKIPEDIA
The Free Encyclopedia

Quantum coin flipping

Consider two remote players, connected by a channel, that don't trust each other. The problem of them agreeing on a random bit by exchanging messages over this channel, without relying on any trusted third party, is called the **coin flipping problem** in cryptography.[1] **Quantum coin flipping** uses the principles of quantum mechanics to encrypt messages for secure communication. It is a cryptographic primitive which can be used to construct more complex and useful cryptographic protocols,[2] e.g. Quantum Byzantine agreement.

Unlike other types of quantum cryptography (in particular, quantum key distribution), quantum coin flipping is a protocol used between two users who do not trust each other.[3] Consequently, both users (or players) want to win the coin toss and will attempt to cheat in various ways.[3]

It is known that if the communication between the players is over a classical channel, i.e. a channel over which quantum information cannot be communicated, then one player can (in principle) always cheat regardless of which protocol is used.[4] We say in principle because it might be that cheating requires an unfeasible amount of computational resource. Under standard computational assumptions, coin flipping can be achieved with classical communication.

The most basic figure of merit for a coin-flipping protocol is given by its bias, a number between 0 and $1/2$. The bias of a protocol captures the success probability of an all-powerful cheating player who uses the best conceivable strategy. A protocol with bias 0 means that no player can cheat. A protocol with bias $1/2$ means that at least one player can always succeed at cheating. Obviously, the smaller the bias better the protocol.

When the communication is over a quantum channel, it has been shown that even the best conceivable protocol can not have a bias less than $1/\sqrt{2} - 1/2 \approx 0.2071$.[5][6]

Consider the case where each player knows the preferred bit of the other. A coin flipping problem which makes this additional assumption constitutes the weaker variant thereof called **weak coin flipping** (WCF). In the case of classical channels this extra assumption yields no improvement. On the other hand, it has been proven that WCF protocols with arbitrarily small biases do exist.[7][8] However, the best known explicit WCF protocol has bias $1/6 \approx 0.1667$.[9]

Although quantum coin flipping offers clear advantages over its classical counterpart in theory, accomplishing it in practice has proven difficult.[3][10]

History

Theory

Manuel Blum introduced coin flipping as part of a classical system in 1983 based on computational algorithms and assumptions.[11] Blum's version of coin flipping answers the following cryptographic problem:

> Alice and Bob are recently divorced, living in two separate cities, and want to decide who gets to keep the car. To decide, Alice wants to flip a coin over the telephone. However, Bob is concerned that if he were to tell Alice heads, she would flip the coin and automatically tell him that he lost.[12]

Thus, the problem with Alice and Bob is that they do not trust each other; the only resource they have is the telephone communication channel, and there is not a third party available to read the coin. Therefore, Alice and Bob must be either truthful and agree on a value or be convinced that the other is cheating.[12]

In 1984, quantum cryptography emerged from a paper written by Charles H. Bennett and Giles Brassard. In this paper, the two introduced the idea of using quantum mechanics to enhance previous cryptographic protocols such as coin flipping.[3] Since then, many researchers have applied quantum mechanics to cryptography as they have proven theoretically to be more secure than classical cryptography, however, demonstrating these protocols in practical systems is difficult to accomplish.

Experiment

As published in 2014, a group of scientists at the Laboratory for Communication and Processing of Information (LTCI) in Paris have implemented quantum coin flipping protocols experimentally.[3] The researchers have reported that the protocol performs better than a classical system over a suitable distance for a metropolitan area optical network.[3]

Definition

Coin flipping

In cryptography, *coin flipping* is defined to be the problem where two mutually distrustful and remote players want to agree on a random bit without relying on any third party.[1]

Strong coin flipping

In quantum cryptography, *strong coin flipping* (SCF) is defined to be a coin flipping problem where each player is oblivious to the preference of the other.[13]

Weak coin flipping

In quantum cryptography, *weak coin flipping* (WCF) is defined to be a coin flipping problem where each player knows the preference of the other.[14]

It follows that the players have opposite preferences. If this were not the case then the problem will be pointless as the players can simply choose the outcome they desire.

Bias

Consider any coin flipping protocol. Let Alice and Bob be the two players who wish to implement the protocol. Consider the scenario where Alice cheats using her best strategy against Bob who honestly follows the protocol. Let the probability that Bob obtains the outcome Alice preferred be given by P_A^*. Consider the reversed situation, i.e. Bob cheats using his best strategy against Alice who honestly follows the protocol. Let the corresponding probability that Alice obtains the outcome Bob preferred to be given by P_B^*.

The bias of the protocol is defined to be $\epsilon := \max[P_A^*, P_B^*] - \frac{1}{2}$.

The half is subtracted because a player will get the desired value half the time purely by chance.

Extensions

Coin flipping can be defined for biased coins as well, i.e. the bits are not equally likely. The notion of correctness has also been formalized which requires that when both players follow the protocol (nobody cheats) the players always agree on the bit generated and that the bit follows some fixed probability distribution.

Protocols

Using conjugate encoding

Quantum coin flipping and other types of quantum cryptography communicate information through the transmission of qubits. The accepting player does not know the information in the qubit until he performs a measurement.[12] Information about each qubit is stored on and carried by a single photon.[10] Once the receiving player measures the photon, it is altered, and will not produce the same output if measured again.[10] Since a photon can only be read the same way once, any other party attempting to intercept the message is easily detectable.[10]

Quantum coin flipping is when random qubits are generated between two players that do not trust each other because both of them want to win the coin toss, which could lead them to cheat in a variety of ways.[3] The essence of coin flipping occurs when the two players issue a sequence of instructions over a communication channel that then eventually results in an output.[10]

A basic quantum coin flipping protocol involves two people: Alice and Bob.[11]

1. Alice sends Bob a set number of K photon pulses in the quantum states $|\phi_{\alpha_i c_i}\rangle$. Each of these photon pulses is independently prepared following a random choice by Alice of basis α_i and bit c_i where i = 1, 2, 3...K.
2. Bob then measures the pulses from Alice by identifying a random basis β_i. Bob records these photons and then reports back the first successfully measured photon j to Alice along

with a random bit *b*.

3. Alice reveals the basis and bit that she used at the basis Bob gave her. If the two bases and bits match, then both parties are truthful and can exchange information. If the bit reported by Bob is different than that of Alice's, one is not being truthful.

A more general explanation of the above protocol is as follows:[15]



Alice decides her random basis and sequence of qubits. She then sends the qubits as photons to Bob via the quantum channel. Bob detects these qubits and records his results in a table. Based on the table, Bob makes his guess to Alice on what basis she used.

1. Alice first chooses a random basis (such as diagonally) and a sequence of random qubits. Alice then encodes her chosen qubits as a sequence of photons following the chosen basis. She then sends these qubits as a train of polarized photons to Bob through the communication channel.
2. Bob chooses a sequence of reading bases randomly for each individual photon. He then reads the photons and records the results in two tables. One table is of the rectilinear (horizontal or vertical) received photons and one of the diagonally received photons. Bob may have holes in his tables due to losses in his detectors or in the transmission channels. Bob now makes a guess as to which basis Alice used and announces his guess to Alice. If he guessed correctly, he wins and if not, he loses.
3. Alice reports whether he won or not by announcing what basis she used to Bob. Alice then confirms the information by sending Bob her entire original qubit sequence that she used in step 1.
4. Bob compares Alice's sequence with his tables to confirm that no cheating occurred on Alice's part. The tables should correspond to Alice's basis and there should be no correlation with the other table.

Assumptions

There are a few assumptions that must be made for this protocol to work properly. The first is that Alice can create each state independent of Bob, and with an equal probability. Second, for the first bit that Bob successfully measures, his basis and bit are both random and completely independent of Alice. The last assumption, is that when Bob measures a state, he has a uniform probability to measure each state, and no state is easier to be detected than others. This last assumption is especially important because if Alice were aware of Bob's inability to measure certain states, she could use that to her advantage.[11]

Cheating

The key issue with coin flipping is that it occurs between two distrustful parties.[15] These two parties are communicating through the communication channel some distance from each other and they have to agree on a winner or loser with each having a 50 percent chance of winning.[15] However, since they are distrustful of one another, cheating is likely to occur. Cheating can occur in a number of ways such as claiming they lost some of the message when they do not like the result or increasing the average number of photons contained in each of the pulses.[3]

For Bob to cheat, he would have to be able to guess Alice's basis with a probability greater than $\frac{1}{2}$.[15] In order to accomplish this, Bob would have to be able to determine a train of photons randomly polarized in one basis from a train of photons polarized in another basis.[15]

Alice, on the other hand, could cheat in a couple of different ways, but she has to be careful because Bob could easily detect it.[15] When Bob sends a correct guess to Alice, she could convince Bob that her photons are actually polarized the opposite of Bob's correct guess.[15] Alice could also send Bob a different original sequence than she actually used in order to beat Bob.[15]

Detecting a third-party

Single photons are used to pass the information from one player to the other (qubits).[10] In this protocol, the information is encoded in the single photons with polarization directions of 0, 45, 90, and 135 degrees, non-orthogonal quantum states.[15] When a third party attempts to read or gain information on the transmission, they alter the photon's polarization in a random way that is likely detected by the two players because it does not match the pattern exchanged between the two legitimate users.[15]

The Dip Dip Boom protocol (weak coin flipping with bias $1/6$)

The Dip Dip Boom (DDB) protocol is a quantum version of the following game.[9] Consider a list of numbers p_i, each between 0 and 1. The players, Alice and Bob, take turns to say "Dip" or "Boom" with probability p_i at round i. The player who says "Boom" wins. Obviously, a cheating player can simply say "Boom" and win as there are no rewards for longer games. We will consider games that terminate so that for some (large) i, say n, we set $p_i = 1$.

Consider round i. Let us denote by $P_A(i)$ and $P_B(i)$ the probability of, respectively, Alice and Bob winning. Let $P_U(i)$ be the probability that the game remains undecided. These numbers for the classical game described above can be evaluated inductively.

We now describe the quantum version. Let $\mathcal{A}, \mathcal{B}$ be a three dimensional Hilbert space spanned by $|A\rangle, |B\rangle, |U\rangle$. Let $\mathcal{M}$ be a two dimensional Hilbert space which is spanned by $|\mathbf{DIP}\rangle, |\mathbf{BOOM}\rangle$.

1. *Initialisation*: Alice holds the $\mathcal{A} \otimes \mathcal{M}$ registers and initialises the state to $|U\rangle \otimes |\mathbf{DIP}\rangle$. Bob holds the register $\mathcal{B}$ and initialises it to the state $|U\rangle$.
2. *Iteration*: For $i = 1$ to n the following must be performed. For odd i we set X=A (for Alice) and Y=B (for Bob); for even i we set X=B and Y=A.
   - X implements the operation $R_i := \mathbf{Rot}(|U\rangle \otimes |\mathbf{DIP}\rangle, |X\rangle \otimes |\mathbf{BOOM}\rangle, p_i)$.
   - X sends the message register to Y.
   - Y implements the operation $\tilde{R}_i := \mathbf{Rot}\left(|U\rangle \otimes |\mathbf{BOOM}\rangle, |X\rangle \otimes |\mathbf{DIP}\rangle, \frac{p_i P_U(i-1)}{P_X(i)}\right)$.
   - Y measures the message register in the computational basis. If the outcome is BOOM then Y aborts and declares him/herself the winner.
3. *Measurement*: Alice and Bob both measure their local register $\mathcal{A}$ and $\mathcal{B}$ respectively. If the outcome is U then they declare themselves to be the winner. If the outcome is A then Alice is the winner and for B it is Bob.

Remarks

- To obtain a balanced protocol one must choose the p_is such that $P_A(n) = \frac{1}{2} = P_B(n)$.

- If both players follow the protocol, i.e. no player cheats, then the outcome at the end of step two will never be BOOM and neither will the outcome at step 3 be $|U\rangle$.
- The bias analysis of this protocol uses SDP duality.
- For large n the bias of the protocol can be made arbitrarily close to $1/6$.

Optimal strong coin flipping

It has been shown that using a WCF protocol with an arbitrarily small bias one can construct a SCF protocol with bias arbitrarily close to $\frac{1}{\sqrt{2}} - \frac{1}{2}$ which is known to be optimal.[16]

Experimental implementation

Using conjugate encoding

As mentioned in the history section, scientists at the LTCI in Paris have experimentally carried out a quantum coin flipping protocol. Previous protocols called for a single photon source or an entangled source to be secure. However, these sources are why it is difficult for quantum coin flipping to be implemented. Instead, the researchers at LTCI used the effects of quantum superposition rather than a single photon source, which they claim makes implementation easier with the standard photon sources available.[3]

The researchers used the Clavis2 platform developed by IdQuantique for their protocol, but needed to modify the Clavis2 system in order for it to work for the coin flipping protocol. The experimental setup they used with the Clavis2 system, involves a two-way approach. Light pulsed at 1550 nanometres is sent from Bob to Alice. Alice then uses a phase modulator to encrypt the information. After encryption, she then uses a Faraday mirror to reflect and attenuate the pulses at her chosen level and sends them back to Bob. Using two high quality single photon detectors, Bob chooses a measurement basis in his phase modulator to detect the pulses from Alice.[11]

They replaced the detectors on Bob's side because of the low detection efficiencies of the previous detectors. When they replaced the detectors, they were able to show a quantum advantage on a channel for over 15 kilometres (9.3 mi). A couple of other challenges the group faced was reprogramming the system because photon source attenuation was high and performing system analyses to identify losses and errors in system components. With these corrections, the scientists were capable of implementing a coin flipping protocol by introducing a small honest abort probability, the probability that two honest participants cannot obtain a coin flip at the end of the protocol, but at a short communication distance.[3]

References

1. Blum, Manuel (1983-01-01). "Coin flipping by telephone a protocol for solving impossible problems" (https://doi.org/10.1145%2F1008908.1008911). *ACM SIGACT News*. **15** (1): 23–27. doi:10.1145/1008908.1008911 (https://doi.org/10.1145%2F1008908.1008911). ISSN 0163-5700 (https://search.worldcat.org/issn/0163-5700). S2CID 19928725 (https://api.semanticscholar.org/CorpusID:19928725).

2. Oded., Goldreich (2003). *Foundations of cryptography*. Cambridge, UK: Cambridge University Press. ISBN 9780521791724. OCLC 45093786 (https://search.worldcat.org/oclc/45093786).
3. Stuart Mason Dambort, "Heads or tails: Experimental quantum coin flipping cryptography performs better than classical protocols" (https://phys.org/news/2014-05-tails-experimental-quantum-coin-flipping.html), *Phys.org*, March 26, 2014
4. Cleve, R. (1986-11-01). "Limits on the security of coin flips when half the processors are faulty" (http://dl.acm.org/citation.cfm?id=12130.12168). *Proceedings of the eighteenth annual ACM symposium on Theory of computing - STOC '86*. ACM. pp. 364–369. doi:10.1145/12130.12168 (https://doi.org/10.1145%2F12130.12168). ISBN 0897911938. S2CID 17394663 (https://api.semanticscholar.org/CorpusID:17394663).
5. A. Kitaev, Quantum Coin Flipping, Quantum Information Processing Workshop, Mathematical Sciences Research Institute, University of California, Berkeley, 2003.
6. Ambainis, A.; Buhrman, H.; Dodis, Y.; Rohrig, H. (2004). "Multiparty quantum coin flipping" (https://ieeexplore.ieee.org/document/1313848). *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004*. IEEE. pp. 250–259. arXiv:quant-ph/0304112 (https://arxiv.org/abs/quant-ph/0304112). doi:10.1109/ccc.2004.1313848 (https://doi.org/10.1109%2Fccc.2004.1313848). ISBN 0769521207. S2CID 3261413 (https://api.semanticscholar.org/CorpusID:3261413).
7. C. Mochon, Quantum Weak Coin Flipping with Arbitrarily Small Bias, preprint, arXiv:0711.4114, 2007.
8. Aharonov, Dorit; Chailloux, André; Ganz, Maor; Kerenidis, Iordanis; Magnin, Loïck (January 2016). "A Simpler Proof of the Existence of Quantum Weak Coin Flipping with Arbitrarily Small Bias". *SIAM Journal on Computing*. **45** (3): 633–679. arXiv:1402.7166 (https://arxiv.org/abs/1402.7166). doi:10.1137/14096387x (https://doi.org/10.1137%2F14096387x). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397). S2CID 7519640 (https://api.semanticscholar.org/CorpusID:7519640).
9. Mochon, Carlos (2005). "Large family of quantum weak coin-flipping protocols". *Physical Review A*. **72** (2): 022341. arXiv:quant-ph/0502068 (https://arxiv.org/abs/quant-ph/0502068). Bibcode:2005PhRvA..72b2341M (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72b2341M). doi:10.1103/PhysRevA.72.022341 (https://doi.org/10.1103%2FPhysRevA.72.022341). S2CID 46533337 (https://api.semanticscholar.org/CorpusID:46533337).
10. Vivek R and Dr. J. Roopchand, "Emerging Trends in Quantum Cryptography – A Survey" (http://www.ijcta.com/documents/volumes/vol3issue4/ijcta2012030417.pdf), *International Journal of Computer Technology and Applications*, August 2012
11. Anna Pappa et al., "Experimental Plug and Play Quantum Coin Flipping" (http://www.nature.com/articles/ncomms4717), *Nature Communications*, April 24, 2014
12. C. Döscher and M. Keyl, "An Introduction to Quantum Coin-Tossing", *Cornell University Library*, February 1, 2008
13. D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, Quantum bit escrow, in Proceedings of the 32nd Annual ACM Symposium on Theory of Computing, ACM, New York, 2000, pp. 705–714.
14. Spekkens, R. W. (2002). "Quantum Protocol for Cheat-Sensitive Weak Coin Flipping". *Physical Review Letters*. **89** (22): 227901. arXiv:quant-ph/0202118 (https://arxiv.org/abs/quant-ph/0202118). Bibcode:2002PhRvL..89v7901S (https://ui.adsabs.harvard.edu/abs/2002PhRvL..89v7901S). doi:10.1103/PhysRevLett.89.227901 (https://doi.org/10.1103%2FPhysRevLett.89.227901). PMID 12485105 (https://pubmed.ncbi.nlm.nih.gov/12485105). S2CID 42694366 (https://api.semanticscholar.org/CorpusID:42694366).
15. Charles H. Bennett and Giles Brassard, "Quantum cryptography: Public key distribution and coin tossing" (http://www.sciencedirect.com/science/article/pii/S0304397514004241?np=y&npKey=9d7c391743e27ff2d85b36896983c21b907525570b2ae94fadb8c09ad21600ca), *Theoretical Computer Science*, December 4, 2014

16. *50th Annual IEEE Symposium on Foundations of Computer Science, 2009 FOCS '09; 25-27 Oct. 2009, Atlanta, Georgia, USA; proceedings*. IEEE Computer Society Technical Committee on Mathematical Foundations of Computing, Annual IEEE Symposium on Foundations of Computer Science 50 2009.10.25-27 Atlanta, Ga., FOCS 50 2009.10.25-27 Atlanta, Ga. Piscataway, NJ. 2009. ISBN 9781424451166. OCLC 838170374 (https://search.worldcat.org/oclc/838170374).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_coin_flipping&oldid=1230111970"

WIKIPEDIA
The Free Encyclopedia

Quantum money

A **quantum money** scheme is a quantum cryptographic protocol that creates and verifies banknotes that are resistant to forgery. It is based on the principle that quantum states cannot be perfectly duplicated (the no-cloning theorem), making it impossible to forge quantum money by including quantum systems in its design.

The concept was first proposed by Stephen Wiesner circa 1970 (though it remained unpublished until 1983),[1] and later influenced the development of quantum key distribution protocols used in quantum cryptography.

Wiesner's quantum money scheme

Wiesner's quantum money scheme was first published in 1983.[1] A formal proof of security, using techniques from semidefinite programming, was given in 2013.[2]

In addition to a unique serial number on each bank note (these notes are actually more like cheques, since a verification step with the bank is required for each transaction), there is a series of isolated two-state quantum systems.[3] For example, photons in one of four polarizations could be used: at 0°, 45°, 90° and 135° to some axis, which is referred to as the vertical. Each of these is a two-state system in one of two bases: the horizontal basis has states with polarizations at 0° and 90° to the vertical, and the diagonal basis has states at 45° and 135° to the vertical.

At the bank, there is a record of all the polarizations and the corresponding serial numbers. On the bank note, the serial number is printed, but the polarizations are kept secret. Thus, whilst the bank can always verify the polarizations by measuring the polarization of each photon in the correct basis without introducing any disturbance, a would-be counterfeiter ignorant of the bases cannot create a copy of the photon polarization states, since even if he knows the two bases, if he chooses the wrong one to measure a photon, it will change the polarization of the photon in the trap, and the forged banknote created will be with this wrong polarization.

For each photon, the would-be counterfeiter has a probability $3/4$ of success in duplicating it correctly. If the total number of photons on the bank note is N, a duplicate will have probability $(3/4)^N$ of passing the bank's verification test. If N is large, this probability becomes exponentially small. The fact that a quantum state cannot be copied is ultimately guaranteed by its proof by the no-cloning theorem, which underlies the security of this system.

Practical implementations

At this time, quantum money is not practical to implement with current technology because the quantum bank notes require to store the quantum states in a quantum memory. Quantum memories can currently store quantum states only for a very short time.

See also

- Hidden Matching Problem

References

1. Wiesner, Stephen (1983-01-01). "Conjugate Coding". *SIGACT News*. **15** (1): 78–88. doi:10.1145/1008908.1008920 (https://doi.org/10.1145%2F1008908.1008920). ISSN 0163-5700 (https://search.worldcat.org/issn/0163-5700). S2CID 207155055 (https://api.semanticscholar.org/CorpusID:207155055).
2. Molina, Abel; Vidick, Thomas; Watrous, John (2013). "Optimal Counterfeiting Attacks and Generalizations for Wiesner's Quantum Money" (https://authors.library.caltech.edu/65494/2/1202.4010.pdf) (PDF). *Theory of Quantum Computation, Communication, and Cryptography (TQC 2012)*. Springer, Berlin, Heidelberg. pp. 45–64. doi:10.1007/978-3-642-35656-8_4 (https://doi.org/10.1007%2F978-3-642-35656-8_4).
3. Lo, Spiller & Popescu, *Introduction to Quantum computation and information* (1998) pp. 81–83

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_money&oldid=1214757516"

WIKIPEDIA
The Free Encyclopedia

Quantum key distribution

Quantum key distribution (**QKD**) is a secure communication method that implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which then can be used to encrypt and decrypt messages. The process of quantum key distribution is not to be confused with quantum cryptography, as it is the best-known example of a quantum-cryptographic task.

An important and unique property of quantum key distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e., the eavesdropper has no information about it). Otherwise no secure key is possible, and communication is aborted.

The security of encryption that uses quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography, which relies on the computational difficulty of certain mathematical functions, and cannot provide any mathematical proof as to the actual complexity of reversing the one-way functions used. QKD has provable security based on information theory, and forward secrecy.

The main drawback of quantum-key distribution is that it usually relies on having an authenticated classical channel of communication. In modern cryptography, having an authenticated classical channel means that one already has exchanged either a symmetric key of sufficient length or public keys of sufficient security level. With such information already available, in practice one can achieve authenticated and sufficiently secure communication without using QKD, such as by using the Galois/Counter Mode of the Advanced Encryption Standard. Thus QKD does the work of a stream cipher at many times the cost.

Quantum key distribution is used to produce and distribute only a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key.[1] In real-world situations, it is often also used with encryption using symmetric key algorithms like the Advanced Encryption Standard algorithm.

Quantum key exchange

Quantum communication involves encoding information in quantum states, or qubits, as opposed to classical communication's use of bits. Usually, photons are used for these quantum states. Quantum key distribution exploits certain properties of these quantum states to ensure its security. There are several different approaches to quantum key distribution, but they can be divided into two main categories depending on which property they exploit.

Prepare and measure protocols

In contrast to classical physics, the act of measurement is an integral part of quantum mechanics. In general, measuring an unknown quantum state changes that state in some way. This is a consequence of quantum indeterminacy and can be exploited in order to detect any eavesdropping on communication (which necessarily involves measurement) and, more importantly, to calculate the amount of information that has been intercepted.

Entanglement based protocols

The quantum states of two (or more) separate objects can become linked together in such a way that they must be described by a combined quantum state, not as individual objects. This is known as entanglement and means that, for example, performing a measurement on one object affects the other. If an entangled pair of objects is shared between two parties, anyone intercepting either object alters the overall system, revealing the presence of the third party (and the amount of information they have gained).

These two approaches can each be further divided into three families of protocols: discrete variable, continuous variable and distributed phase reference coding. Discrete variable protocols were the first to be invented, and they remain the most widely implemented. The other two families are mainly concerned with overcoming practical limitations of experiments. The two protocols described below both use discrete variable coding.

BB84 protocol: Charles H. Bennett and Gilles Brassard (1984)

This protocol, known as BB84 after its inventors and year of publication, was originally described using photon polarization states to transmit the information.[2] However, any two pairs of conjugate states can be used for the protocol, and many optical-fibre-based implementations described as BB84 use phase encoded states. The sender (traditionally referred to as Alice) and the receiver (Bob) are connected by a quantum communication channel which allows quantum states to be transmitted. In the case of photons this channel is generally either an optical fibre or simply free space. In addition they communicate via a public classical channel, for example using broadcast radio or the internet. The protocol is designed with the assumption that an eavesdropper (referred to as Eve) can interfere in any way with the quantum channel, while the classical channel needs to be authenticated.[3][4]

The security of the protocol comes from encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot in general be measured without disturbing the original state (see *No-cloning theorem*). BB84 uses two pairs of states, with each pair conjugate to the other pair, and the two states within a pair orthogonal to each other. Pairs of orthogonal states are referred to as a basis. The usual polarization state pairs used are either the rectilinear basis of vertical (0°) and horizontal (90°), the diagonal basis of 45° and 135° or the circular basis of left- and right-handedness. Any two of these bases are conjugate to each other, and so any two can be used in the protocol. Below the rectilinear and diagonal bases are used.

Basis	0	1
+	↕	→
×	↗	↘

The first step in BB84 is quantum transmission. Alice creates a random bit (0 or 1) and then randomly selects one of her two bases (rectilinear or diagonal in this case) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis, as shown in the adjacent table. So for example a 0 is encoded in the rectilinear basis (+) as a vertical polarization state, and a 1 is encoded in the diagonal basis (x) as a 135° state. Alice then transmits a single photon in the state specified to Bob, using the quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent.

According to quantum mechanics (particularly quantum indeterminacy), no possible measurement distinguishes between the 4 different polarization states, as they are not all orthogonal. The only possible measurement is between any two orthogonal states (an orthonormal basis). So, for example, measuring in the rectilinear basis gives a result of horizontal or vertical. If the photon was created as horizontal or vertical (as a rectilinear eigenstate) then this measures the correct state, but if it was created as 45° or 135° (diagonal eigenstates) then the rectilinear measurement instead returns either horizontal or vertical at random. Furthermore, after this measurement the photon is polarized in the state it was measured in (horizontal or vertical), with all information about its initial polarization lost.

As Bob does not know the basis the photons were encoded in, all he can do is to select a basis at random to measure in, either rectilinear or diagonal. He does this for each photon he receives, recording the time, measurement basis used and measurement result. After Bob has measured all the photons, he communicates with Alice over the public classical channel. Alice broadcasts the basis each photon was sent in, and Bob the basis each was measured in. They both discard photon measurements (bits) where Bob used a different basis, which is half on average, leaving half the bits as a shared key.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↕	→	↘	↕	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↕	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

To check for the presence of an eavesdropper, Alice and Bob now compare a predetermined subset of their remaining bit strings. If a third party (usually referred to as Eve, for "eavesdropper") has gained any information about the photons' polarization, this introduces errors in Bob's measurements. Other environmental conditions can cause errors in a similar fashion. If more than p bits differ they abort the key and try again, possibly with a different quantum channel, as the security of the key cannot be guaranteed. p is chosen so that if the number of bits known to Eve is less than this, privacy amplification can be used to reduce Eve's knowledge of the key to an arbitrarily small amount at the cost of reducing the length of the key.

E91 protocol: Artur Ekert (1991)

Artur Ekert's scheme[5] uses entangled pairs of photons. These can be created by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair.

The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. This necessitates that the two distant parties have exact directionality synchronization. However, the particular results are completely random; it is impossible for Alice to predict if she (and thus Bob) will get vertical polarization or horizontal polarization. Second, any attempt at eavesdropping by Eve destroys these correlations in a way that Alice and Bob can detect.

Similarly to BB84, the protocol involves a private measurement protocol before detecting the presence of Eve. The measurement stage involves Alice measuring each photon she receives using some basis from the set $Z_0, Z_{\frac{\pi}{8}}, Z_{\frac{\pi}{4}}$ while Bob chooses from $Z_0, Z_{\frac{\pi}{8}}, Z_{-\frac{\pi}{8}}$ where Z_θ is the $\{|\uparrow\rangle, |\rightarrow\rangle\}$ basis rotated by θ. They keep their series of basis choices private until measurements are completed. Two groups of photons are made: the first consists of photons measured using the same basis by Alice and Bob while the second contains all other photons. To detect eavesdropping, they can compute the test statistic S using the correlation coefficients between Alice's bases and Bob's similar to that shown in the Bell test experiments. Maximally entangled photons would result in $|S| = 2\sqrt{2}$. If this were not the case, then Alice and Bob can conclude Eve has introduced local realism to the system, violating Bell's theorem. If the protocol is successful, the first group can be used to generate keys since those photons are completely anti-aligned between Alice and Bob.

Device-independent quantum key distribution

In traditional QKD, the quantum devices used must be perfectly calibrated, trustworthy, and working exactly as they are expected to.[6] Deviations from expected measurements can be extremely hard to detect, which leaves the entire system vulnerable. A new protocol called device independent QKD (DIQKD) or measurement device independent QKD (MDIQKD) allows for the use of uncharacterized or untrusted devices, and for deviations from expected measurements to be included in the overall system.[6][7] These deviations will cause the protocol to abort when detected, rather than resulting in incorrect data.[6]

DIQKD was first proposed by Mayers and Yao,[8] building off of the BB84 protocol. They presented that in DIQKD, the quantum device, which they refer to as the photon source, be manufactured to come with tests that can be run by Alice and Bob to "self-check" if their device is working properly. Such a test would only need to consider the classical inputs and outputs in order to determine how much information is at risk of being intercepted by Eve. A self checking, or "ideal" source would not have to be characterized,[7][9] and would therefore not be susceptible to implementation flaws.[7]

Recent research has proposed using a Bell test to check that a device is working properly.[6] Bell's theorem ensures that a device can create two outcomes that are exclusively correlated, meaning that Eve could not intercept the results, without making any assumptions about said device. This requires highly entangled states, and a low quantum bit error rate.[7] DIQKD presents difficulties in creating qubits that are in such high quality entangled states, which makes it a challenge to realize experimentally.[6]

Twin fields quantum key distribution

Twin fields quantum key distribution (TFQKD) was introduced in 2018, and is a version of DIQKD designed to overcome the fundamental rate-distance limit of traditional quantum key distribution.[10] The rate-distance limit, also known as the rate-loss trade off, describes how as distance increases between Alice and Bob, the rate of key generation decreases exponentially.[11] In traditional QKD protocols, this decay has been eliminated via the addition of physically secured relay nodes, which can be placed along the quantum link with the intention of dividing it up into several low-loss sections. Researchers have also recommended the use of quantum repeaters, which when added to the relay nodes make it so that they no longer need to be physically secured.[11] Quantum repeaters, however, are difficult to create and have yet to be implemented on a useful scale.[10] TFQKD aims to bypass the rate-distance limit without the use of quantum repeaters or relay nodes, creating manageable levels of noise and a process that can be repeated much more easily with today's existing technology.[10]

The original protocol for TFQKD is as follows: Alice and Bob each have a light source and one arm on an interferometer in their laboratories. The light sources create two dim optical pulses with a randomly phase p_a or p_b in the interval [0, 2π) and an encoding phase γ_a or γ_b. The pulses are sent along a quantum to Charlie, a third party who can be malicious or not. Charlie uses a beam splitter to overlap the two pulses and perform a measurement. He has two detectors in his own lab, one of which will light up if the bits are equal (00) or (11), and the other when they are different (10, 01). Charlie will announce to Alice and Bob which of the detectors lit up, at which point they publicly reveal the phases p and γ.[10] This is different from traditional QKD, in which the phases used are never revealed.[12]

Information reconciliation and privacy amplification

The quantum key distribution protocols described above provide Alice and Bob with nearly identical shared keys, and also with an estimate of the discrepancy between the keys. These differences can be caused by eavesdropping, but also by imperfections in the transmission line and detectors. As it is impossible to distinguish between these two types of errors, guaranteed security requires the assumption that all errors are due to eavesdropping. Provided the error rate between the keys is lower than a certain threshold (27.6% as of 2002[13]), two steps can be performed to first remove the erroneous bits and then reduce Eve's knowledge of the key to an arbitrary small value. These two steps are known as **information reconciliation** and **privacy amplification** respectively, and were first described in 1988.[14]

Information reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimise the information sent about each key, as this can be read by Eve. A common protocol used for information reconciliation is the **cascade protocol**, proposed in 1994.[15] This operates in several rounds, with both keys divided into blocks in each round and the parity of those blocks compared. If a difference in parity is found then a binary search is performed to find and correct the error. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively, which is the source of the cascade name. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. At the end of multiple rounds Alice and Bob have identical keys with high probability; however, Eve has additional information about the key from the parity information exchanged. However, from a coding theory point of view information reconciliation is essentially source coding with side information. In consequence any coding scheme that works for this problem can be used for information reconciliation. Lately turbocodes,[16] LDPC codes[17] and polar codes[18] have been used for this purpose improving the efficiency of the cascade protocol.

Privacy amplification is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possible parity information). Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This is performed using a randomness extractor, for example, by applying a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated, based on how much information Eve could have gained about the old key (which is known due to the errors this would introduce), in order to reduce the probability of Eve having any knowledge of the new key to a very low value.

Implementations

Experimental

In 1991, John Rarity, Paul Tapster and Artur Ekert, researchers from the UK Defence Research Agency in Malvern and Oxford University, demonstrated quantum key distribution protected by the violation of the Bell inequalities.

In 2008, exchange of secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre), was achieved by a collaboration between the University of Cambridge and Toshiba using the BB84 protocol with decoy state pulses.[19]

In 2007, Los Alamos National Laboratory/NIST achieved quantum key distribution over a 148.7 km of optic fibre using the BB84 protocol.[20] Significantly, this distance is long enough for almost all the spans found in today's fibre networks. A European collaboration achieved free space QKD over 144 km between two of the Canary Islands using entangled photons (the Ekert scheme) in 2006,[21] and using BB84 enhanced with decoy states[22][23][24][25][26] in 2007.[27]

As of August 2015 the longest distance for optical fiber (307 km)[28] was achieved by University of Geneva and Corning Inc. In the same experiment, a secret key rate of 12.7 kbit/s was generated, making it the highest bit rate system over distances of 100 km. In 2016 a team from Corning and various institutions in China achieved a distance of 404 km, but at a bit rate too slow to be practical.[29]

In June 2017, physicists led by Thomas Jennewein at the Institute for Quantum Computing and the University of Waterloo in Waterloo, Canada achieved the first demonstration of quantum key distribution from a ground transmitter to a moving aircraft. They reported optical links with distances between 3–10 km and generated secure keys up to 868 kilobytes in length.[30]

Also in June 2017, as part of the Quantum Experiments at Space Scale project, Chinese physicists led by Pan Jianwei at the University of Science and Technology of China measured entangled photons over a distance of 1203 km between two ground stations, laying the groundwork for future intercontinental quantum key distribution experiments.[31] Photons were sent from one ground station to the satellite they had named *Micius* and back down to another ground station, where they "observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions" along a "summed length varying from 1600 to 2400 kilometers."[32] Later that year BB84 was successfully implemented over satellite links from *Micius* to ground stations in China and Austria. The keys were combined and the result was used to transmit images and video between Beijing, China, and Vienna, Austria.[33]

In August 2017, a group at Shanghai Jiaotong University experimentally demonstrate that polarization quantum states including general qubits of single photon and entangled states can survive well after travelling through seawater,[34] representing the first step towards underwater quantum communication.

In May 2019 a group led by Hong Guo at Peking University and Beijing University of Posts and Telecommunications reported field tests of a continuous-variable QKD system through commercial fiber networks in Xi'an and Guangzhou over distances of 30.02 km (12.48 dB) and 49.85 km (11.62 dB) respectively.[35]

In December 2020, Indian Defence Research and Development Organisation tested a QKD between two of its laboratories in Hyderabad facility. The setup also demonstrated the validation of detection of a third party trying to gain knowledge of the communication. Quantum based security against eavesdropping was validated for the deployed system at over 12 km (7.5 mi) range and 10 dB attenuation over fibre optic channel. A continuous wave laser source was used to generate photons without depolarization effect and timing accuracy employed in the setup was of the order of picoseconds. The Single photon avalanche detector (SPAD) recorded arrival of photons and key rate was achieved in the range of kbps with low Quantum bit error rate.[36]

In March 2021, Indian Space Research Organisation also demonstrated a free-space Quantum Communication over a distance of 300 meters. A free-space QKD was demonstrated at Space Applications Centre (SAC), Ahmedabad, between two line-of-sight buildings within the campus for video conferencing by quantum-key encrypted signals. The experiment utilised a NAVIC receiver for time synchronization between the transmitter and receiver modules. Later in January 2022, Indian scientists were able to successfully create an atmospheric channel for exchange of crypted messages and images. After demonstrating quantum communication between two ground stations, India has plans to develop Satellite Based Quantum Communication (SBQC).[37][38]

In July 2022, researchers published their work experimentally implementing a device-independent quantum key distribution (DIQKD) protocol that uses quantum entanglement (as suggested by Ekert)[5] to insure resistance to quantum hacking attacks.[6] They were able to create two ions, about two meters apart that were in a high quality entangled state using the following process: Alice and Bob each have ion trap nodes with an $^{88}Sr^{+}$ qubit inside. Initially, they excite the ions to an electronic state, which creates an entangled state. This process also creates two photons, which are then captured and transported using an optical fiber, at which point a Bell-basis measurement is performed and the ions are projected to a highly entangled state. Finally the qubits are returned to new locations in the ion traps disconnected from the optical link so that no information can be leaked. This is repeated many times before the key distribution proceeds.[6]

A separate experiment published in July 2022 demonstrated implementation of DIQKD that also uses a Bell inequality test to ensure that the quantum device is functioning, this time at a much larger distance of about 400m, using an optical fiber 700m long.[7] The set up for the experiment was similar to the one in the paragraph above, with some key differences. Entanglement was generated in a quantum network link (QNL) between two ^{87}Rb atoms in separate laboratories located 400m apart, connected by the 700m channel.The atoms are entangled by electronic excitation, at which point two photons are generated and collected, to be sent to the bell state measurement (BSM) setup. The photons are projected onto a $|\psi^{+}$ state, indicating maximum entanglement. The rest of the key exchange protocol used is similar to the original QKD protocol, with the only difference being that keys are generated with two measurement settings instead of one.[7]

Since the proposal of Twin Field Quantum Key Distribution in 2018, a myriad of experiments have been performed with the goal of increasing the distance in a QKD system. The most successful of which was able to distribute key information across a distance of 833.8 km.[12]

In 2023, Scientists at Indian Institute of Technology (IIT) Delhi have achieved a trusted-node-free quantum key distribution (QKD) up to *380 km* in standard telecom fiber with a very low quantum bit error rate (QBER).[39]

Commercial

Many companies around the world offer commercial quantum key distribution, for example: ID Quantique (Geneva), MagiQ Technologies, Inc. (New York), QNu Labs (Bengaluru, India), QuintessenceLabs (Australia), QRate (Russia), SeQureNet (Paris), Quantum Optics Jena (Germany) and KEEQuant (https://www.keequant.com) (Germany). Several other companies also have active research programs, including KETS Quantum Security (UK), Toshiba, HP, IBM, Mitsubishi, NEC and NTT (See External links for direct research links).

In 2004, the world's first bank transfer using quantum key distribution was carried out in Vienna, Austria.[40] Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capital in the national election

occurring on 21 October 2007.[41] In 2013, Battelle Memorial Institute installed a QKD system built by ID Quantique between their main campus in Columbus, Ohio and their manufacturing facility in nearby Dublin.[42] Field tests of Tokyo QKD network have been underway for some time.[43]

Quantum key distribution networks

DARPA

The DARPA Quantum Network,[44] was a 10-node quantum key distribution network, which ran continuously for four years, 24 hours a day, from 2004 to 2007 in Massachusetts in the United States. It was developed by BBN Technologies, Harvard University, Boston University, with collaboration from IBM Research, the National Institute of Standards and Technology, and QinetiQ. It supported a standards-based Internet computer network protected by quantum key distribution.

SECOQC

The world's first computer network protected by quantum key distribution was implemented in October 2008, at a scientific conference in Vienna. The name of this network is SECOQC (**Se**cure **Co**mmunication Based on **Q**uantum **C**ryptography) and the EU funded this project. The network used 200 km of standard fibre-optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west.[45]

SwissQuantum

Id Quantique has successfully completed the longest running project for testing Quantum Key Distribution (QKD) in a field environment. The main goal of the SwissQuantum network project installed in the Geneva metropolitan area in March 2009, was to validate the reliability and robustness of QKD in continuous operation over a long time period in a field environment. The quantum layer operated for nearly 2 years until the project was shut down in January 2011 shortly after the initially planned duration of the test.

Chinese networks

In May 2009, a hierarchical quantum network was demonstrated in Wuhu, China. The hierarchical network consisted of a backbone network of four nodes connecting a number of subnets. The backbone nodes were connected through an optical switching quantum router. Nodes within each subnet were also connected through an optical switch, which were connected to the backbone network through a trusted relay.[46]

Launched in August 2016, the QUESS space mission created an international QKD channel between China and the Institute for Quantum Optics and Quantum Information in Vienna, Austria − a ground distance of 7,500 km (4,700 mi), enabling the first intercontinental secure quantum video call.[47][48][49] By October 2017, a 2,000-km fiber line was operational between Beijing, Jinan, Hefei and Shanghai.[50]

Together they constitute the world's first space-ground quantum network.[51] Up to 10 Micius/QUESS satellites are expected,[52] allowing a European–Asian quantum-encrypted network by 2020, and a global network by 2030.[53][54]

Tokyo QKD Network

The Tokyo QKD Network[55] was inaugurated on the first day of the UQCC2010 conference. The network involves an international collaboration between 7 partners; NEC, Mitsubishi Electric, NTT and NICT from Japan, and participation from Europe by Toshiba Research Europe Ltd. (UK), Id Quantique (Switzerland) and All Vienna (Austria). "All Vienna" is represented by researchers from the Austrian Institute of Technology (AIT), the Institute for Quantum Optics and Quantum Information (IQOQI) and the University of Vienna.

Los Alamos National Laboratory

A hub-and-spoke network has been operated by Los Alamos National Laboratory since 2011. All messages are routed via the hub. The system equips each node in the network with quantum transmitters —i.e., lasers—but not with expensive and bulky photon detectors. Only the hub receives quantum messages. To communicate, each node sends a one-time pad to the hub, which it then uses to communicate securely over a classical link. The hub can route this message to another node using another one time pad from the second node. The entire network is secure only if the central hub is secure. Individual nodes require little more than a laser: Prototype nodes are around the size of a box of matches.[56]

Singapore's National Quantum-Safe Network Plus (NQSN+)

National Quantum-Safe Network Plus (NQSN+) was launched by IMDA in 2023 and is part of Singapore’s Digital Connectivity Blueprint, which outlines the next bound of Singapore’s digital connectivity to 2030. NQSN+ will support network operators to deploy quantum-safe networks nationwide, granting businesses easy access to quantum-safe solutions that safeguard their critical data. The NQSN+ will start with two network operators, Singtel and SPTel, together with SpeQtral. Each will build a nationwide, interoperable quantum-safe network that can serve all businesses. Businesses can work with NQSN+ operators to integrate quantum-safe solutions such as Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) and be secure in the quantum age.[57]

Eagle-1

In 2024, the ESA plans to launch the satellite Eagle-1, an experimental space-based quantum key distribution system.[58]

Attacks and security proofs

Intercept and resend

The simplest type of possible attack is the intercept-resend attack, where Eve measures the quantum states (photons) sent by Alice and then sends replacement states to Bob, prepared in the state she measures. In the BB84 protocol, this produces errors in the key Alice and Bob share. As Eve has no knowledge of the basis a state sent by Alice is encoded in, she can only guess which basis to measure in, in the same way as Bob. If she chooses correctly, she measures the correct photon polarization state as sent by Alice, and resends the correct state to Bob. However, if she chooses incorrectly, the state she measures is random, and the state sent to Bob cannot be the same as the state sent by Alice. If Bob then measures this state in the same basis Alice sent, he too gets a random result—as Eve has sent him a state in the opposite basis—with a 50% chance of an erroneous result (instead of the correct result he would get without the presence of Eve). The table below shows an example of this type of attack.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↕	→	↘	↕	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↕	↗	→	↕	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↕	↗	↗	↘	→	↗	↕	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✘			✓		✓

The probability Eve chooses the incorrect basis is 50% (assuming Alice chooses randomly), and if Bob measures this intercepted photon in the basis Alice sent he gets a random result, i.e., an incorrect result with probability of 50%. The probability an intercepted photon generates an error in the key string is then 50% × 50% = 25%. If Alice and Bob publicly compare n of their key bits (thus discarding them as key bits, as they are no longer secret) the probability they find disagreement and identify the presence of Eve is

$$P_d = 1 - \left(\frac{3}{4}\right)^n$$

So to detect an eavesdropper with probability $P_d = 0.999999999$ Alice and Bob need to compare $n = 72$ key bits.

Man-in-the-middle attack

Quantum key distribution is vulnerable to a man-in-the-middle attack when used without authentication to the same extent as any classical protocol, since no known principle of quantum mechanics can distinguish friend from foe. As in the classical case, Alice and Bob cannot authenticate each other and establish a secure connection without some means of verifying each other's identities (such as an initial shared secret). If Alice and Bob have an initial shared secret then they can use an unconditionally secure authentication scheme (such as Carter-Wegman,[59]) along with quantum key distribution to exponentially expand this key, using a small amount of the new key to authenticate the next session.[60] Several methods to create this initial shared secret have been proposed, for example using a 3rd party[61] or chaos theory.[62] Nevertheless, only "almost strongly universal" family of hash functions can be used for unconditionally secure authentication.[63]

Photon number splitting attack

In the BB84 protocol Alice sends quantum states to Bob using single photons. In practice many implementations use laser pulses attenuated to a very low level to send the quantum states. These laser pulses contain a very small number of photons, for example 0.2 photons per pulse, which are distributed according to a Poisson distribution. This means most pulses actually contain no photons (no pulse is sent), some pulses contain 1 photon (which is desired) and a few pulses contain 2 or more photons. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. This is the basis of the photon number splitting attack,[64] where Eve stores these extra photons in a quantum memory until Bob detects the remaining single photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors.

Even with the possibility of a PNS attack a secure key can still be generated, as shown in the GLLP security proof;[65] however, a much higher amount of privacy amplification is needed reducing the secure key rate significantly (with PNS the rate scales as t^2 as compared to t for a single photon sources, where t is the transmittance of the quantum channel).

There are several solutions to this problem. The most obvious is to use a true single photon source instead of an attenuated laser. While such sources are still at a developmental stage QKD has been carried out successfully with them.[66] However, as current sources operate at a low efficiency and frequency key rates and transmission distances are limited. Another solution is to modify the BB84 protocol, as is done for example in the SARG04 protocol,[67] in which the secure key rate scales as $t^{3/2}$. The most promising solution is the decoy states[22][23][24][25][26] in which Alice randomly sends some of her laser pulses with a lower average photon number. These decoy states can be used to detect a PNS attack, as Eve has no way to tell which pulses are signal and which decoy. Using this idea the secure key rate scales as t, the

same as for a single photon source. This idea has been implemented successfully first at the University of Toronto,[68][69] and in several follow-up QKD experiments,[70] allowing for high key rates secure against all known attacks.

Denial of service

Because currently a dedicated fibre optic line (or line of sight in free space) is required between the two points linked by quantum key distribution, a denial of service attack can be mounted by simply cutting or blocking the line. This is one of the motivations for the development of quantum key distribution networks, which would route communication via alternate links in case of disruption.

Trojan-horse attacks

A quantum key distribution system may be probed by Eve by sending bright light into the quantum channel and analyzing the back-reflections in a Trojan-horse attack. In a recent research study it has been shown that Eve discerns Bob's secret basis choice with higher than 90% probability, breaching the security of the system.[71]

Security proofs

If Eve is assumed to have unlimited resources, for example both classical and quantum computing power, there are many more attacks possible. BB84 has been proven secure against any attacks allowed by quantum mechanics, both for sending information using an ideal photon source which only ever emits a single photon at a time,[72] and also using practical photon sources which sometimes emit multiphoton pulses.[65] These proofs are unconditionally secure in the sense that no conditions are imposed on the resources available to the eavesdropper; however, there are other conditions required:

1. Eve cannot physically access Alice and Bob's encoding and decoding devices.
2. The random number generators used by Alice and Bob must be trusted and truly random (for example a Quantum random number generator).
3. The classical communication channel must be authenticated using an unconditionally secure authentication scheme.
4. The message must be encrypted using one-time pad like scheme

Quantum hacking

Hacking attacks target vulnerabilities in the operation of a QKD protocol or deficiencies in the components of the physical devices used in construction of the QKD system. If the equipment used in quantum key distribution can be tampered with, it could be made to generate keys that were not secure using a random number generator attack. Another common class of attacks is the Trojan horse attack[73] which does not require physical access to the endpoints: rather than attempt to read Alice and Bob's single photons, Eve sends a large pulse of light back to Alice in between transmitted photons. Alice's equipment reflects some of Eve's light, revealing the state of Alice's basis (e.g., a polarizer). This attack can be detected, e.g. by using a classical detector to check the non-legitimate signals (i.e. light from Eve) entering Alice's system. It is also conjectured that most hacking attacks can similarly be defeated by modifying the implementation, though there is no formal proof.

Several other attacks including faked-state attacks,[74] phase remapping attacks,[75] and time-shift attacks[76] are now known. The time-shift attack has even been demonstrated on a commercial quantum cryptosystem.[77] This is the first demonstration of quantum hacking against a non-homemade quantum key distribution system. Later on, the phase-remapping attack was also demonstrated on a specially configured, research oriented open QKD system (made and provided by the Swiss company Id Quantique under their Quantum Hacking program).[78] It is one of the first 'intercept-and-resend' attacks on top of a widely used QKD implementation in commercial QKD systems. This work has been widely reported in media.[79][80][81][82]

The first attack that claimed to be able to eavesdrop the whole key[83] without leaving any trace was demonstrated in 2010. It was experimentally shown that the single-photon detectors in two commercial devices could be fully remote-controlled using specially tailored bright illumination. In a spree of publications[84][85][86] thereafter, the collaboration between the Norwegian University of Science and Technology in Norway and Max Planck Institute for the Science of Light in Germany, has now demonstrated several methods to successfully eavesdrop on commercial QKD systems based on weaknesses of avalanche photodiodes (APDs) operating in gated mode. This has sparked research on new approaches to securing communications networks.[87]

Counterfactual quantum key distribution

The task of distributing a secret key could be achieved even when the particle (on which the secret information, e.g. polarization, has been encoded) does not traverse through the quantum channel using a protocol developed by Tae-Gon Noh.[88] Here Alice generates a photon which, by not taking a measurement until later, exists in a superposition of being in paths (a) and (b) simultaneously. Path (a) stays inside Alice's secure device and path (b) goes to Bob. By rejecting the photons that Bob receives and only accepting the ones he doesn't receive, Bob & Alice can set up a secure channel, i.e. Eve's attempts to read the *counterfactual* photons would still be detected. This protocol uses the quantum phenomenon whereby the possibility that a photon can be sent has an effect even when it is not sent. So-called interaction-free measurement also uses this quantum effect, as for example in the bomb testing problem, whereby an experimenter can conceptually determine which bombs are not duds without setting them off, except in a counterfactual sense.

History

Quantum cryptography was proposed first by Stephen Wiesner, then at Columbia University in New York, who, in the early 1970s, introduced the concept of quantum conjugate coding. His seminal paper titled "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78–88, 1983). In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded. He illustrated his idea with a design of unforgeable bank notes. A decade later, building upon this work, Charles H. Bennett, of the IBM Thomas J. Watson Research Center, and Gilles Brassard, of the University of Montreal, proposed a

method for secure communication based on Wiesner's "conjugate observables". In 1990, Artur Ekert, then a PhD student at Wolfson College, University of Oxford, developed a different approach to quantum key distribution based on quantum entanglement.

Future

The current commercial systems are aimed mainly at governments and corporations with high security requirements. Key distribution by courier is typically used in such cases, where traditional key distribution schemes are not believed to offer enough guarantee. This has the advantage of not being intrinsically distance limited, and despite long travel times the transfer rate can be high due to the availability of large capacity portable storage devices. The major difference of quantum key distribution is the ability to detect any interception of the key, whereas with courier the key security cannot be proven or tested. QKD (quantum key distribution) systems also have the advantage of being automatic, with greater reliability and lower operating costs than a secure human courier network.

Kak's three-stage protocol has been proposed as a method for secure communication that is entirely quantum unlike quantum key distribution in which the cryptographic transformation uses classical algorithms.[89]

Factors preventing wide adoption of quantum key distribution outside high security areas include the cost of equipment, and the lack of a demonstrated threat to existing key exchange protocols. However, with optic fibre networks already present in many countries the infrastructure is in place for a more widespread use.

An Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) has been set up to address standardisation issues in quantum cryptography.[90]

European Metrology Institutes, in the context of dedicated projects,[91][92] are developing measurements required to characterise components of QKD systems.

Toshiba Europe has been awarded a prestigious Institute of Physics Award for Business Innovation. This recognises Toshiba's pioneering QKD[93] technology developed over two decades of research, protecting communication infrastructure from present and future cyber-threats, and commercialising UK-manufactured products which pave the road to the quantum internet.

Toshiba also took the Semi Grand Prix award in the Solutions Category for the QKD has won the Minister of Economy, Trade and Industry Award in CEATEC AWARD 2021, the prestigious awards presented at CEATEC, Japan's premier electronics industry trade show.[94]

Deprecation from governmental institutions

Some organizations have recommended using "post-quantum cryptography (or quantum-resistant cryptography)" as an alternative because of the problems it raises in practical use. For example, the US National Security Agency, European Union Agency for Cybersecurity of EU (ENISA), National Cyber Security Centre (United Kingdom), and French Secretariat for Defense and Security (ANSSI) recommend it. (read through the bibliography for details).[95][96][97][98]

For example, the US National Security Agency addresses five issues:[95]

1. Quantum key distribution is only a partial solution. QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.
2. Quantum key distribution requires special purpose equipment. QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.
3. Quantum key distribution increases infrastructure costs and insider threat risks. QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.
4. Securing and validating quantum key distribution is a significant challenge. The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.[99]
5. Quantum key distribution increases the risk of denial of service. The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

In response to problem 1 above, attempts to deliver authentication keys using post-quantum cryptography (or quantum-resistant cryptography) have been proposed worldwide. On the other hand, quantum-resistant cryptography is cryptography belonging to the class of computational security. In 2015, a research result was already published that "sufficient care must be taken in implementation to achieve information-theoretic security for the system as a whole when authentication keys that are not information-theoretic secure are used" (if the authentication key is not information-theoretically secure, an attacker can break it to bring all classical and quantum communications under control and relay them to launch a man-in-the-middle attack).[100] Ericsson, a private company, also cites and points out the above problems and then presents a report that it may not be able to support the zero trust security model, which is a recent trend in network security technology.[101]

See also

- List of quantum key distribution protocols
- Quantum computing
- Quantum cryptography
- Quantum information science

- Quantum network

References

1. Shannon, C. E. (1949). "Communication Theory of Secrecy Systems*". *Bell System Technical Journal*. **28** (4). Institute of Electrical and Electronics Engineers (IEEE): 656–715. doi:10.1002/j.1538-7305.1949.tb00928.x (https://doi.org/10.1002%2Fj.1538-7305.1949.tb00928.x). hdl:10338.dmlcz/119717 (https://hdl.handle.net/10338.dmlcz%2F119717). ISSN 0005-8580 (https://search.worldcat.org/issn/0005-8580).
2. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
3. Tomamichel, Marco; Leverrier, Anthony (2017). "A largely self-contained and complete security proof for quantum key distribution". *Quantum*. **1**: 14. arXiv:1506.08458 (https://arxiv.org/abs/1506.08458). Bibcode:2017Quant...1...14T (https://ui.adsabs.harvard.edu/abs/2017Quant...1...14T). doi:10.22331/q-2017-07-14-14 (https://doi.org/10.22331%2Fq-2017-07-14-14). S2CID 56465385 (https://api.semanticscholar.org/CorpusID:56465385).
4. Portmann, Christopher; Renner, Renato (2014). "Cryptographic security of quantum key distribution". arXiv:1409.3525 (https://arxiv.org/abs/1409.3525) [quant-ph (https://arxiv.org/archive/quant-ph)].
5. Ekert, Artur K. (5 August 1991). "Quantum cryptography based on Bell's theorem". *Physical Review Letters*. **67** (6): 661–663. Bibcode:1991PhRvL..67..661E (https://ui.adsabs.harvard.edu/abs/1991PhRvL..67..661E). doi:10.1103/PhysRevLett.67.661 (https://doi.org/10.1103%2FPhysRevLett.67.661). PMID 10044956 (https://pubmed.ncbi.nlm.nih.gov/10044956). S2CID 27683254 (https://api.semanticscholar.org/CorpusID:27683254).
6. Nadlinger, D. P.; Drmota, P.; Nichol, B. C.; Araneda, G.; Main, D.; Srinivas, R.; Lucas, D. M.; Ballance, C. J.; Ivanov, K.; Tan, E. Y.-Z.; Sekatski, P.; Urbanke, R. L.; Renner, R.; Sangouard, N.; Bancal, J.-D. (July 2022). "Experimental quantum key distribution certified by Bell's theorem" (https://www.nature.com/articles/s41586-022-04941-5). *Nature*. **607** (7920): 682–686. arXiv:2109.14600 (https://arxiv.org/abs/2109.14600). Bibcode:2022Natur.607..682N (https://ui.adsabs.harvard.edu/abs/2022Natur.607..682N). doi:10.1038/s41586-022-04941-5 (https://doi.org/10.1038%2Fs41586-022-04941-5). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 35896644 (https://pubmed.ncbi.nlm.nih.gov/35896644). S2CID 251131731 (https://api.semanticscholar.org/CorpusID:251131731).
7. Zhang, Wei; van Leent, Tim; Redeker, Kai; Garthoff, Robert; Schwonnek, René; Fertig, Florian; Eppelt, Sebastian; Rosenfeld, Wenjamin; Scarani, Valerio; Lim, Charles C.-W.; Weinfurter, Harald (July 2022). "A device-independent quantum key distribution system for distant users" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9329124). *Nature*. **607** (7920): 687–691. arXiv:2110.00575 (https://arxiv.org/abs/2110.00575). Bibcode:2022Natur.607..687Z (https://ui.adsabs.harvard.edu/abs/2022Natur.607..687Z). doi:10.1038/s41586-022-04891-y (https://doi.org/10.1038%2Fs41586-022-04891-y). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9329124 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9329124). PMID 35896650 (https://pubmed.ncbi.nlm.nih.gov/35896650).
8. Mayers, Dominic; Yao, Andrew (14 September 1998). "Quantum Cryptography with Imperfect Apparatus". arXiv:quant-ph/9809039 (https://arxiv.org/abs/quant-ph/9809039).

9. Schwonnek, René; Goh, Koon Tong; Primaatmaja, Ignatius W.; Tan, Ernest Y.-Z.; Wolf, Ramona; Scarani, Valerio; Lim, Charles C.-W. (17 May 2021). "Device-independent quantum key distribution with random key basis" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8128898). *Nature Communications*. **12** (1): 2880. arXiv:2005.02691 (https://arxiv.org/abs/2005.02691). Bibcode:2021NatCo..12.2880S (https://ui.adsabs.harvard.edu/abs/2021NatCo..12.2880S). doi:10.1038/s41467-021-23147-3 (https://doi.org/10.1038%2Fs41467-021-23147-3). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 8128898 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8128898). PMID 34001885 (https://pubmed.ncbi.nlm.nih.gov/34001885).
10. Lucamarini, M.; Yuan, Z. L.; Dynes, J. F.; Shields, A. J. (May 2018). "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters" (https://www.nature.com/articles/s41586-018-0066-6). *Nature*. **557** (7705): 400–403. arXiv:1811.06826 (https://arxiv.org/abs/1811.06826). Bibcode:2018Natur.557..400L (https://ui.adsabs.harvard.edu/abs/2018Natur.557..400L). doi:10.1038/s41586-018-0066-6 (https://doi.org/10.1038%2Fs41586-018-0066-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 29720656 (https://pubmed.ncbi.nlm.nih.gov/29720656). S2CID 256768464 (https://api.semanticscholar.org/CorpusID:256768464).
11. Takeoka, Masahiro; Guha, Saikat; Wilde, Mark M. (24 October 2014). "Fundamental rate-loss tradeoff for optical quantum key distribution" (https://doi.org/10.1038%2Fncomms6235). *Nature Communications*. **5** (1): 5235. arXiv:1504.06390 (https://arxiv.org/abs/1504.06390). Bibcode:2014NatCo...5.5235T (https://ui.adsabs.harvard.edu/abs/2014NatCo...5.5235T). doi:10.1038/ncomms6235 (https://doi.org/10.1038%2Fncomms6235). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMID 25341406 (https://pubmed.ncbi.nlm.nih.gov/25341406).
12. Wang, Shuang; Yin, Zhen-Qiang; He, De-Yong; Chen, Wei; Wang, Rui-Qiang; Ye, Peng; Zhou, Yao; Fan-Yuan, Guan-Jie; Wang, Fang-Xiang; Chen, Wei; Zhu, Yong-Gang; Morozov, Pavel V.; Divochiy, Alexander V.; Zhou, Zheng; Guo, Guang-Can (February 2022). "Twin-field quantum key distribution over 830-km fibre" (https://www.nature.com/articles/s41566-021-00928-2). *Nature Photonics*. **16** (2): 154–161. Bibcode:2022NaPho..16..154W (https://ui.adsabs.harvard.edu/abs/2022NaPho..16..154W). doi:10.1038/s41566-021-00928-2 (https://doi.org/10.1038%2Fs41566-021-00928-2). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893). S2CID 117167883 (https://api.semanticscholar.org/CorpusID:117167883).
13. Chau, H.F. (2002). "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate" (https://journals.aps.org/pra/pdf/10.1103/PhysRevA.66.060302). *Physical Review A*. **66** (6): 60302. Bibcode:2002PhRvA..66f0302C (https://ui.adsabs.harvard.edu/abs/2002PhRvA..66f0302C). doi:10.1103/PhysRevA.66.060302 (https://doi.org/10.1103%2FPhysRevA.66.060302). hdl:10722/43370 (https://hdl.handle.net/10722%2F43370). Retrieved 4 September 2020.
14. Bennett, C. H.; Brassard, J. M.; Robert (1988). "Privacy Amplification by Public Discussion" (https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=594dfbdf3e3ba9df94a31ab9cb1e23912773b98a). *SIAM J. Comput*. **17** (2): 210–229. doi:10.1137/0217014 (https://doi.org/10.1137%2F0217014).
15. Brassard, G.; Salvail, L. (1993). "Secret-key reconciliation by public discussion" (https://link.springer.com/chapter/10.1007/3-540-48285-7_35). *Workshop on the Theory and Application of Cryptographic Techniques*. Springer. pp. 410–423. doi:10.1007/3-540-48285-7_35 (https://doi.org/10.1007%2F3-540-48285-7_35). ISBN 3-540-48285-7.
16. Nguyen, Kim-Chi; Van Assche, Gilles; Cerf, Nicolas J. (10–13 October 2004). "Side-Information Coding with Turbo Codes and its Application to Quantum Key Distribution". arXiv:cs/0406001 (https://arxiv.org/abs/cs/0406001). Parma, Italy.

17. Elkouss, D.; Martinez-Mateo, J.; Martin, V. (2010). "Information reconciliation for quantum key distribution" (https://web.archive.org/web/20131215041349/http://www.dma.fi.upm.es/jmartinez/doc/qic-11-34_0226-0238.pdf) (PDF). *Quantum Information & Computation*. **11**: 226–238. doi:10.26421/QIC11.3-4-3 (https://doi.org/10.26421%2FQIC11.3-4-3). Archived from the original (http://www.dma.fi.upm.es/jmartinez/doc/qic-11-34_0226-0238.pdf) (PDF) on 15 December 2013. Retrieved 4 September 2020.
18. Nguyen, Kim-Chi; Gilles Van Assche; Cerf, Nicolas J. (2012). "High Performance Error Correction for Quantum Key Distribution using Polar Codes". arXiv:1204.5882v3 (https://arxiv.org/abs/1204.5882v3) [quant-ph (https://arxiv.org/archive/quant-ph)].
19. Dixon, A.R.; Z.L. Yuan; Dynes, J.F.; Sharpe, A. W.; Shields, A. J. (2008). "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate". *Optics Express*. **16** (23): 18790–7. arXiv:0810.1069 (https://arxiv.org/abs/0810.1069). Bibcode:2008OExpr..1618790D (https://ui.adsabs.harvard.edu/abs/2008OExpr..1618790D). doi:10.1364/OE.16.018790 (https://doi.org/10.1364%2FOE.16.018790). PMID 19581967 (https://pubmed.ncbi.nlm.nih.gov/19581967). S2CID 17141431 (https://api.semanticscholar.org/CorpusID:17141431).
20. Hiskett, P A; Rosenberg, D; Peterson, C G; Hughes, R J; Nam, S; Lita, A E; Miller, A J; Nordholt, J E (14 September 2006). "Long-distance quantum key distribution in optical fibre" (https://doi.org/10.1088%2F1367-2630%2F8%2F9%2F193). *New Journal of Physics*. **8** (9). IOP Publishing: 193. arXiv:quant-ph/0607177 (https://arxiv.org/abs/quant-ph/0607177). Bibcode:2006NJPh....8..193H (https://ui.adsabs.harvard.edu/abs/2006NJPh....8..193H). doi:10.1088/1367-2630/8/9/193 (https://doi.org/10.1088%2F1367-2630%2F8%2F9%2F193). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).
21. Ursin, Rupert; Tiefenbacher, Felix; Schmitt-Manderbach, T.; Weier, H.; Scheidl, T.; Lindenthal, M.; Blauensteiner, B.; Jennewein, T.; Perdigues, J.; Trojek, P.; Ömer, B.; Fürst, M.; Meyenburg, M.; Rarity, J.; Sodnik, Z.; Barbieri, C.; Weinfurter, H.; Zeilinger, A. (2006). "Entanglement-based quantum communication over 144 km km". *Nature Physics*. **3** (7): 481–486. arXiv:quant-ph/0607182 (https://arxiv.org/abs/quant-ph/0607182). Bibcode:2006quant.ph..7182U (https://ui.adsabs.harvard.edu/abs/2006quant.ph..7182U). doi:10.1038/nphys629 (https://doi.org/10.1038%2Fnphys629). S2CID 108284907 (https://api.semanticscholar.org/CorpusID:108284907).
22. Hwang, Won-Young (1 August 2003). "Quantum Key Distribution with High Loss: Toward Global Secure Communication". *Physical Review Letters*. **91** (5): 057901. arXiv:quant-ph/0211153 (https://arxiv.org/abs/quant-ph/0211153). Bibcode:2003PhRvL..91e7901H (https://ui.adsabs.harvard.edu/abs/2003PhRvL..91e7901H). doi:10.1103/physrevlett.91.057901 (https://doi.org/10.1103%2Fphysrevlett.91.057901). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 12906634 (https://pubmed.ncbi.nlm.nih.gov/12906634). S2CID 19225674 (https://api.semanticscholar.org/CorpusID:19225674).
23. H.-K. Lo, in Proceedings of 2004 IEEE ISIT (IEEE Press, New York, 2004), p. 137
24. Wang, Xiang-Bin (16 June 2005). "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography". *Physical Review Letters*. **94** (23): 230503. arXiv:quant-ph/0410075 (https://arxiv.org/abs/quant-ph/0410075). Bibcode:2005PhRvL..94w0503W (https://ui.adsabs.harvard.edu/abs/2005PhRvL..94w0503W). doi:10.1103/physrevlett.94.230503 (https://doi.org/10.1103%2Fphysrevlett.94.230503). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 16090451 (https://pubmed.ncbi.nlm.nih.gov/16090451). S2CID 2651690 (https://api.semanticscholar.org/CorpusID:2651690).
25. H.-K. Lo, X. Ma, K. Chen, "Decoy State Quantum Key Distribution" (https://archive.today/20120712103031/http://prl.aps.org/abstract/PRL/v94/i23/e230504), Physical Review Letters, 94, 230504 (2005)
26. Ma, Xiongfeng; Qi, Bing; Zhao, Yi; Lo, Hoi-Kwong (2005). "Practical decoy state for quantum key distribution". *Physical Review A*. **72** (1): 012326. arXiv:quant-ph/0503005 (https://arxiv.org/abs/quant-ph/0503005). Bibcode:2005PhRvA..72a2326M (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72a2326M). doi:10.1103/PhysRevA.72.012326 (https://doi.org/10.1103%2FPhysRevA.72.012326). S2CID 836096 (https://api.semanticscholar.org/CorpusID:836096).

27. Schmitt-Manderbach, Tobias; Weier, Henning; Fürst, Martin; Ursin, Rupert; Tiefenbacher, Felix; et al. (5 January 2007). "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km" (http://xqp.physik.lmu.de/publications/files/articles_2007/prl_98_010504.pdf) (PDF). *Physical Review Letters*. **98** (1). American Physical Society (APS): 010504. Bibcode:2007PhRvL..98a0504S (https://ui.adsabs.harvard.edu/abs/2007PhRvL..98a0504S). doi:10.1103/physrevlett.98.010504 (https://doi.org/10.1103%2Fphysrevlett.98.010504). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 17358463 (https://pubmed.ncbi.nlm.nih.gov/17358463). S2CID 15102161 (https://api.semanticscholar.org/CorpusID:15102161).
28. Korzh, Boris; Lim, Charles Ci Wen; Houlmann, Raphael; Gisin, Nicolas; Li, Ming Jun; Nolan, Daniel; Sanguinetti, Bruno; Thew, Rob; Zbinden, Hugo (2015). "Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre". *Nature Photonics*. **9** (3): 163–168. arXiv:1407.7427 (https://arxiv.org/abs/1407.7427). Bibcode:2015NaPho...9..163K (https://ui.adsabs.harvard.edu/abs/2015NaPho...9..163K). doi:10.1038/nphoton.2014.327 (https://doi.org/10.1038%2Fnphoton.2014.327). S2CID 59028718 (https://api.semanticscholar.org/CorpusID:59028718).
29. Yin, Juan; Cao, Yuan; Li, Yu-Huai; Liao, Sheng-Kai; Zhang, Liang; Ren, Ji-Gang; Cai, Wen-Qi; Liu, Wei-Yue; Li, Bo; Dai, Hui; et al. (2017). "Satellite-based entanglement distribution over 1200 kilometers". *Science*. **356** (6343): 1140–1144. arXiv:1707.01339 (https://arxiv.org/abs/1707.01339). Bibcode:2017arXiv170701339Y (https://ui.adsabs.harvard.edu/abs/2017arXiv170701339Y). doi:10.1126/science.aan3211 (https://doi.org/10.1126%2Fscience.aan3211). PMID 28619937 (https://pubmed.ncbi.nlm.nih.gov/28619937). S2CID 5206894 (https://api.semanticscholar.org/CorpusID:5206894).
30. Pugh, C. J.; Kaiser, S.; Bourgoin, J.- P.; Jin, J.; Sultana, N.; Agne, S.; Anisimova, E.; Makarov, V.; Choi, E.; Higgins, B. L.; Jennewein, T. (2017). "Airborne demonstration of a quantum key distribution receiver payload". *Quantum Science and Technology*. **2** (2): 024009. arXiv:1612.06396 (https://arxiv.org/abs/1612.06396). Bibcode:2017QS&T....2b4009P (https://ui.adsabs.harvard.edu/abs/2017QS&T....2b4009P). doi:10.1088/2058-9565/aa701f (https://doi.org/10.1088%2F2058-9565%2Faa701f). S2CID 21279135 (https://api.semanticscholar.org/CorpusID:21279135).
31. "China's quantum satellite achieves 'spooky action' at a record distance" (https://www.science.org/content/article/china-s-quantum-satellite-achieves-spooky-action-record-distance). 15 June 2017. Retrieved 15 June 2017.
32. Yin, J.; Cao, Y.; Li, Y.- H.; Liao, S.- K.; Zhang, L.; Ren, J.- G.; Cai, W.- Q.; Liu, W.- Y.; Li, B.; Dai, H.; Li, G.- B.; Lu, Q.- M.; Gong, Y.- H.; Xu, Y.; Li, S.- L.; Li, F.- Z.; Yin, Y.- Y.; Jiang, Z.- Q.; Li, M.; Jia, J.- J.; Ren, G.; He, D.; Zhou, Y.- L.; Zhang, X.- X.; Wang, N.; Chang, X.; Zhu, Z.- C.; Liu, N.- L.; Lu, C.- Y.; Shu, R.; Peng, C.- Z.; Wang, J.- Y.; Pan, J.- W. (2017). "Satellite-based entanglement distribution over 1200 kilometers" (https://doi.org/10.1126%2Fscience.aan3211). *Science*. **356** (6343): 1140–4. arXiv:1707.01339 (https://arxiv.org/abs/1707.01339). doi:10.1126/science.aan3211 (https://doi.org/10.1126%2Fscience.aan3211). PMID 28619937 (https://pubmed.ncbi.nlm.nih.gov/28619937).
33. Liao, Sheng-Kai; Cai, Wen-Qi; Handsteiner, Johannes; Liu, Bo; Yin, Juan; Zhang, Liang; Rauch, Dominik; Fink, Matthias; Ren, Ji-Gang; Liu, Wei-Yue; et al. (2018). "Satellite-Relayed Intercontinental Quantum Network". *Physical Review Letters*. **120** (3): 030501. arXiv:1801.04418 (https://arxiv.org/abs/1801.04418). Bibcode:2018PhRvL.120c0501L (https://ui.adsabs.harvard.edu/abs/2018PhRvL.120c0501L). doi:10.1103/PhysRevLett.120.030501 (https://doi.org/10.1103%2FPhysRevLett.120.030501). PMID 29400544 (https://pubmed.ncbi.nlm.nih.gov/29400544). S2CID 206306725 (https://api.semanticscholar.org/CorpusID:206306725).

34. Ji, Ling; Gao, Jun; Yang, Ai-Lin; Feng, Zhen; Lin, Xiao-Feng; Li, Zhong-Gen; Jin, Xian-Min (2017). "Towards quantum communications in free-space seawater". *Optics Express*. **25** (17): 19795–19806. arXiv:1602.05047 (https://arxiv.org/abs/1602.05047). Bibcode:2017OExpr..2519795J (https://ui.adsabs.harvard.edu/abs/2017OExpr..2519795J). doi:10.1364/OE.25.019795 (https://doi.org/10.1364%2FOE.25.019795). PMID 29041667 (https://pubmed.ncbi.nlm.nih.gov/29041667). S2CID 46757097 (https://api.semanticscholar.org/CorpusID:46757097).
35. Zhang, Yichen; Li, Zhengyu; Chen, Ziyang; Weedbrook, Christian; Zhao, Yijia; Wang, Xiangyu; Huang, Yundi; Xu, Chunchao; Zhang, Xiaoxiong; Wang, Zhenya; Li, Mei; Zhang, Xueying; Zheng, Ziyong; Chu, Binjie; Gao, Xinyu; Meng, Nan; Cai, Weiwen; Wang, Zheng; Wang, Gan; Yu, Song; Guo, Hong (2019). "Continuous-variable QKD over 50 km commercial fiber". *Quantum Science and Technology*. **4** (3): 035006. arXiv:1709.04618 (https://arxiv.org/abs/1709.04618). Bibcode:2019QS&T....4c5006Z (https://ui.adsabs.harvard.edu/abs/2019QS&T....4c5006Z). doi:10.1088/2058-9565/ab19d1 (https://doi.org/10.1088%2F2058-9565%2Fab19d1). S2CID 116403328 (https://api.semanticscholar.org/CorpusID:116403328).
36. Ministry of Defence (9 December 2020). "Quantum Communication between two DRDO Laboratories" (https://pib.gov.in/PressReleasePage.aspx?PRID=1679349). *Press Information Bureau*. Retrieved 22 March 2021.
37. "ISRO makes breakthrough demonstration of free-space Quantum Key Distribution (QKD) over 300 m" (https://web.archive.org/web/20210322164134/https://www.isro.gov.in/update/22-mar-2021/isro-makes-breakthrough-demonstration-of-free-space-quantum-key-distribution-qkd). *Indian Space Research Organisation*. 22 March 2021. Archived from the original (https://www.isro.gov.in/update/22-mar-2021/isro-makes-breakthrough-demonstration-of-free-space-quantum-key-distribution-qkd) on 22 March 2021. Retrieved 22 March 2021.
38. "Department of Space demonstrates entanglement based quantum communication over 300m free space along with real time cryptographic applications" (https://web.archive.org/web/20220201151914/https://www.isro.gov.in/update/31-jan-2022/department-of-space-demonstrates-entanglement-based-quantum-communication-over). *Indian Space Research Organisation*. 31 January 2022. Archived from the original (https://www.isro.gov.in/update/31-jan-2022/department-of-space-demonstrates-entanglement-based-quantum-communication-over) on 1 February 2022. Retrieved 1 February 2022.
39. "EMERGING TECHNOLOGIES: IIT Delhi researchers achieve secure quantum communication for 380 km in standard telecom fiber - EducationTimes.com" (https://www.educationtimes.com/article/campus-beat-college-life/99733828/emerging-technologies-iit-delhi-researchers-achieve-secure-quantum-communication-for-380-km-in-standard-telecom-fiber). *www.educationtimes.com*.
40. http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf Archived (https://web.archive.org/web/20130309095431/http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf) 9 March 2013 at the Wayback Machine *secoqc.net*
41. Jordans, Frank (12 October 2007). "Swiss Call New Vote Encryption System 'Unbreakable' " (https://web.archive.org/web/20071209214958/http://www.technewsworld.com/story/59793.html). technewsworld.com. Archived from the original (http://www.technewsworld.com/story/59793.html) on 9 December 2007. Retrieved 8 March 2013.
42. Dillow, Clay (14 October 2013). "Unbreakable encryption comes to the U.S" (https://web.archive.org/web/20131014104149/http://tech.fortune.cnn.com/2013/10/14/quantum-key/). fortune.cnn.com. Archived from the original (http://tech.fortune.cnn.com/2013/10/14/quantum-key/) on 14 October 2013.

43. Sasaki, M.; et al. (2011). "Field test of quantum key distribution in the Tokyo QKD Network". *Optics Express*. **19** (11): 10387–10409. arXiv:1103.3566 (https://arxiv.org/abs/1103.3566). Bibcode:2011OExpr..1910387S (https://ui.adsabs.harvard.edu/abs/2011OExpr..1910387S). doi:10.1364/OE.19.010387 (https://doi.org/10.1364%2FOE.19.010387). PMID 21643295 (https://pubmed.ncbi.nlm.nih.gov/21643295). S2CID 593516 (https://api.semanticscholar.org/CorpusID:593516).
44. Knight, Will. "Quantum cryptography network gets wireless link" (https://www.newscientist.com/article/dn7484). Retrieved 18 August 2016.
45. " 'Unbreakable' encryption unveiled" (http://news.bbc.co.uk/1/hi/sci/tech/7661311.stm). 9 October 2008. Retrieved 18 August 2016 – via bbc.co.uk.
46. Xu, FangXing; Chen, Wei; Wang, Shuang; Yin, ZhenQiang; Zhang, Yang; Liu, Yun; Zhou, Zheng; Zhao, YiBo; Li, HongWei; Liu, Dong (2009), "Field experiment on a robust hierarchical metropolitan quantum cryptography network", *Chinese Science Bulletin*, **54** (17): 2991–2997, arXiv:0906.3576 (https://arxiv.org/abs/0906.3576), Bibcode:2009ChSBu..54.2991X (https://ui.adsabs.harvard.edu/abs/2009ChSBu..54.2991X), doi:10.1007/s11434-009-0526-3 (https://doi.org/10.1007%2Fs11434-009-0526-3), S2CID 118300112 (https://api.semanticscholar.org/CorpusID:118300112)
47. Lin Xing (16 August 2016). "China launches world's first quantum science satellite" (https://web.archive.org/web/20171201030546/http://physicsworld.com/cws/article/news/2016/aug/16/china-launches-world-s-first-quantum-science-satellite). *Physics World*. Institute of Physics. Archived from the original (http://physicsworld.com/cws/article/news/2016/aug/16/china-launches-world-s-first-quantum-science-satellite) on 1 December 2017. Retrieved 17 August 2016.
48. "First Quantum Satellite Successfully Launched" (https://web.archive.org/web/20180318054341/https://www.oeaw.ac.at/en/events-communication/public-relations-communication/public-relations-communication/ausgewaehlte-oeaw-pressemeldungen/press-releases/first-quantum-satellite-successfully-launched/). *Austrian Academy of Sciences*. 16 August 2016. Archived from the original (http://www.oeaw.ac.at/en/events-communication/public-relations-communication/public-relations-communication/ausgewaehlte-oeaw-pressemeldungen/press-releases/first-quantum-satellite-successfully-launched/) on 18 March 2018. Retrieved 17 August 2016.
49. Wall, Mike (16 August 2016). "China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite" (http://www.space.com/33760-china-launches-quantum-communications-satellite.html). *Space.com*. Purch. Retrieved 17 August 2016.
50. Yuen Yiu (19 January 2018). "Is China the Leader in Quantum Communications?" (https://www.insidescience.org/news/china-leader-quantum-communications). *IEEE*. Retrieved 19 March 2018.
51. Amy Nordrum (3 October 2017). "China Demonstrates Quantum Encryption By Hosting a Video Call" (https://spectrum.ieee.org/china-successfully-demonstrates-quantum-encryption-by-hosting-a-video-call). *IEEE*. Retrieved 17 March 2018.
52. Jian-Wei Pan (3 October 2017). "A quantum communications satellite proved its potential in 2017" (https://www.sciencenews.org/article/global-quantum-communication-top-science-stories-2017-yir). *Science News*. Retrieved 19 March 2018.
53. huaxia (16 August 2016). "China Focus: China's space satellites make quantum leap" (https://web.archive.org/web/20160817155904/http://news.xinhuanet.com/english/2016-08/16/c_135604287.htm). Xinhua. Archived from the original (http://news.xinhuanet.com/english/2016-08/16/c_135604287.htm) on 17 August 2016. Retrieved 17 August 2016.
54. Jeffrey Lin; P.W. Singer; John Costello (3 March 2016). "China's Quantum Satellite Could Change Cryptography Forever" (http://www.popsci.com/chinas-quantum-satellite-could-change-cryptography-forever). *Popular Science*. Retrieved 17 August 2016.
55. "UQCC2010 - Updating Quantum Cryptography and Communications 2010 | Tokyo QKD Network" (http://www.uqcc2010.org/highlights/index.html). *www.uqcc2010.org*.

56. Hughes, Richard J.; Nordholt, Jane E.; McCabe, Kevin P.; Newell, Raymond T.; Peterson, Charles G.; Somma, Rolando D. (2013). "Network-Centric Quantum Communications with Application to Critical Infrastructure Protection". arXiv:1305.0305 (https://arxiv.org/abs/1305.0305) [quant-ph (https://arxiv.org/archive/quant-ph)].
57. Singapore, IMDA (21 August 2024). "Singapore's National Quantum-Safe Network Plus (NQSN+)" (https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/national-quantum-safe-network-plus). *imda.gov.sg*.
58. Jones, Andrew (15 October 2022). "Europe plans to launch a quantum encryption satellite for ultrasecure communications in 2024" (https://www.space.com/europe-quantum-encryption-satellite-planned). *Space.com*.
59. Wegman, Mark N.; Carter, J.Lawrence (1981). "New hash functions and their use in authentication and set equality" (https://doi.org/10.1016%2F0022-0000%2881%2990033-7). *Journal of Computer and System Sciences*. **22** (3). Elsevier BV: 265–279. doi:10.1016/0022-0000(81)90033-7 (https://doi.org/10.1016%2F0022-0000%2881%2990033-7). ISSN 0022-0000 (https://search.worldcat.org/issn/0022-0000).
60. Nguyen, Kim-Chi; Gilles Van Assche; Cerf, Nicolas J. (2007). "Using quantum key distribution for cryptographic purposes: A survey". arXiv:quant-ph/0701168 (https://arxiv.org/abs/quant-ph/0701168).
61. Zhang, Z.; Liu, J.; Wang, D.; Shi, S. (2007). "Quantum direct communication with authentication". *Phys. Rev. A*. **75** (2): 026301. arXiv:quant-ph/0604125 (https://arxiv.org/abs/quant-ph/0604125). Bibcode:2007PhRvA..75b6301Z (https://ui.adsabs.harvard.edu/abs/2007PhRvA..75b6301Z). doi:10.1103/physreva.75.026301 (https://doi.org/10.1103%2Fphysreva.75.026301). S2CID 5529511 (https://api.semanticscholar.org/CorpusID:5529511).
62. D. Huang, Z. Chen, Y. Guo and M. Lee "Quantum Secure Direct Communication Based on Chaos with Authentication", Journal of the Physical Society of Japan Vol. 76 No. 12, 124001 (2007) ("124001" (https://journals.jps.jp/doi/10.1143/JPSJ.76.124001). Retrieved 2 May 2024.)
63. "5. Unconditionally secure authentication" (http://www.lysator.liu.se/~jc/mthesis/5_Unconditionally_secure_au.html). Retrieved 18 August 2016.
64. Brassard, Gilles; Lütkenhaus, Norbert; Mor, Tal; Sanders, Barry C. (7 August 2000). "Limitations on Practical Quantum Cryptography". *Physical Review Letters*. **85** (6). American Physical Society (APS): 1330–1333. arXiv:quant-ph/9911054 (https://arxiv.org/abs/quant-ph/9911054). Bibcode:2000PhRvL..85.1330B (https://ui.adsabs.harvard.edu/abs/2000PhRvL..85.1330B). doi:10.1103/physrevlett.85.1330 (https://doi.org/10.1103%2Fphysrevlett.85.1330). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10991544 (https://pubmed.ncbi.nlm.nih.gov/10991544). S2CID 18688722 (https://api.semanticscholar.org/CorpusID:18688722).
65. D. Gottesman, H.-K. Lo, N. L¨utkenhaus, and J. Preskill, Quant. Inf. Comp. 4, 325 (2004)
66. Intallura, P. M.; Ward, M. B.; Karimov, O. Z.; Yuan, Z. L.; See, P.; et al. (15 October 2007). "Quantum key distribution using a triggered quantum dot source emitting near 1.3μm". *Applied Physics Letters*. **91** (16): 161103. arXiv:0710.0565 (https://arxiv.org/abs/0710.0565). Bibcode:2007ApPhL..91p1103I (https://ui.adsabs.harvard.edu/abs/2007ApPhL..91p1103I). doi:10.1063/1.2799756 (https://doi.org/10.1063%2F1.2799756). ISSN 0003-6951 (https://search.worldcat.org/issn/0003-6951). S2CID 118994015 (https://api.semanticscholar.org/CorpusID:118994015).
67. Scarani, Valerio; Acín, Antonio; Ribordy, Grégoire; Gisin, Nicolas (6 February 2004). "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". *Physical Review Letters*. **92** (5): 057901. arXiv:quant-ph/0211131 (https://arxiv.org/abs/quant-ph/0211131). Bibcode:2004PhRvL..92e7901S (https://ui.adsabs.harvard.edu/abs/2004PhRvL..92e7901S). doi:10.1103/physrevlett.92.057901 (https://doi.org/10.1103%2Fphysrevlett.92.057901). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 14995344 (https://pubmed.ncbi.nlm.nih.gov/14995344). S2CID 4791560 (https://api.semanticscholar.org/CorpusID:4791560).

68. Zhao, Yi; Qi, Bing; Ma, Xiongfeng; Lo, Hoi-Kwong; Qian, Li (22 February 2006). "Experimental Quantum Key Distribution with Decoy States". *Physical Review Letters*. **96** (7). American Physical Society (APS): 070502. arXiv:quant-ph/0503192 (https://arxiv.org/abs/quant-ph/0503192). Bibcode:2006PhRvL..96g0502Z (https://ui.adsabs.harvard.edu/abs/2006PhRvL..96g0502Z). doi:10.1103/physrevlett.96.070502 (https://doi.org/10.1103%2Fphysrevlett.96.070502). hdl:1807/10013 (https://hdl.handle.net/1807%2F10013). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 16606067 (https://pubmed.ncbi.nlm.nih.gov/16606067). S2CID 2564853 (https://api.semanticscholar.org/CorpusID:2564853).
69. Y.Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in Proc. IEEE ISIT, pp. 2094–2098 (2006).
70. Yuan, Z. L.; Sharpe, A. W.; Shields, A. J. (2007). "Unconditionally secure one-way quantum key distribution using decoy pulses". *Applied Physics Letters*. **90** (1). AIP Publishing: 011118. arXiv:quant-ph/0610015 (https://arxiv.org/abs/quant-ph/0610015). Bibcode:2007ApPhL..90a1118Y (https://ui.adsabs.harvard.edu/abs/2007ApPhL..90a1118Y). doi:10.1063/1.2430685 (https://doi.org/10.1063%2F1.2430685). ISSN 0003-6951 (https://search.worldcat.org/issn/0003-6951). S2CID 20424612 (https://api.semanticscholar.org/CorpusID:20424612).
71. Jain, N.; et al. (2014). "Trojan-horse attacks threaten the security of practical quantum cryptography". *New Journal of Physics*. **16** (12): 123030. arXiv:1406.5813 (https://arxiv.org/abs/1406.5813). Bibcode:2014NJPh...16l3030J (https://ui.adsabs.harvard.edu/abs/2014NJPh...16l3030J). doi:10.1088/1367-2630/16/12/123030 (https://doi.org/10.1088%2F1367-2630%2F16%2F12%2F123030). S2CID 15127809 (https://api.semanticscholar.org/CorpusID:15127809).
72. Shor, Peter W.; Preskill, John (10 July 2000). "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol" (https://authors.library.caltech.edu/2745/1/SHOprl00.pdf) (PDF). *Physical Review Letters*. **85** (2): 441–444. arXiv:quant-ph/0003004 (https://arxiv.org/abs/quant-ph/0003004). Bibcode:2000PhRvL..85..441S (https://ui.adsabs.harvard.edu/abs/2000PhRvL..85..441S). doi:10.1103/physrevlett.85.441 (https://doi.org/10.1103%2Fphysrevlett.85.441). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10991303 (https://pubmed.ncbi.nlm.nih.gov/10991303). S2CID 703220 (https://api.semanticscholar.org/CorpusID:703220).
73. Vakhitov, Artem; Makarov, Vadim; Hjelme, Dag R. (2001). "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography". *Journal of Modern Optics*. **48** (13). Informa UK Limited: 2023–2038. Bibcode:2001JMOp...48.2023V (https://ui.adsabs.harvard.edu/abs/2001JMOp...48.2023V). doi:10.1080/09500340108240904 (https://doi.org/10.1080%2F09500340108240904). ISSN 0950-0340 (https://search.worldcat.org/issn/0950-0340). S2CID 16173055 (https://api.semanticscholar.org/CorpusID:16173055).
74. Makarov *, Vadim; Hjelme, Dag R. (20 March 2005). "Faked states attack on quantum cryptosystems". *Journal of Modern Optics*. **52** (5). Informa UK Limited: 691–705. Bibcode:2005JMOp...52..691M (https://ui.adsabs.harvard.edu/abs/2005JMOp...52..691M). doi:10.1080/09500340410001730986 (https://doi.org/10.1080%2F09500340410001730986). ISSN 0950-0340 (https://search.worldcat.org/issn/0950-0340). S2CID 17478135 (https://api.semanticscholar.org/CorpusID:17478135).
75. Fung, Chi-Hang Fred; Qi, Bing; Tamaki, Kiyoshi; Lo, Hoi-Kwong (12 March 2007). "Phase-remapping attack in practical quantum-key-distribution systems". *Physical Review A*. **75** (3): 032314. arXiv:quant-ph/0601115 (https://arxiv.org/abs/quant-ph/0601115). Bibcode:2007PhRvA..75c2314F (https://ui.adsabs.harvard.edu/abs/2007PhRvA..75c2314F). doi:10.1103/physreva.75.032314 (https://doi.org/10.1103%2Fphysreva.75.032314). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 15024401 (https://api.semanticscholar.org/CorpusID:15024401).
76. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 43 (2007)

77. Zhao, Yi; Fung, Chi-Hang Fred; Qi, Bing; Chen, Christine; Lo, Hoi-Kwong (28 October 2008). "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems". *Physical Review A*. **78** (4): 042333. arXiv:0704.3253 (https://arxiv.org/abs/0704.3253). Bibcode:2008PhRvA..78d2333Z (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78d2333Z). doi:10.1103/physreva.78.042333 (https://doi.org/10.1103%2Fphysreva.78.042333). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 117595905 (https://api.semanticscholar.org/CorpusID:117595905).
78. F. Xu, B. Qi, and H.-K. Lo, New J. Phys. 12, 113026 (2010)
79. Quantum crypto boffins in successful backdoor sniff – Erroneous error-handling undermines bulletproofness (https://www.theregister.co.uk/2010/05/18/quantum_crypto_attack/) retrieved 2010-05-26
80. Merali, Zeeya (20 May 2010). "Quantum crack in cryptographic armour" (http://www.nature.com/news/2010/100520/full/news.2010.256.html). *Nature*. doi:10.1038/news.2010.256 (https://doi.org/10.1038%2Fnews.2010.256). Retrieved 18 August 2016 – via www.nature.com.
81. "Light fantastic" (http://www.economist.com/node/16681905). *The Economist*. 26 July 2010.
82. "Quantum cryptography system hacked - physicsworld.com" (https://web.archive.org/web/20111108030705/http://physicsworld.com/cws/article/news/42667). Archived from the original (http://physicsworld.com/cws/article/news/42667) on 8 November 2011. Retrieved 26 July 2011.
83. Lydersen, Lars; Wiechers, Carlos; Wittmann, Christoffer; Elser, Dominique; Skaar, Johannes; Makarov, Vadim (29 August 2010). "Hacking commercial quantum cryptography systems by tailored bright illumination". *Nature Photonics*. **4** (10). Springer Science and Business Media LLC: 686–689. arXiv:1008.4593 (https://arxiv.org/abs/1008.4593). Bibcode:2010NaPho...4..686L (https://ui.adsabs.harvard.edu/abs/2010NaPho...4..686L). doi:10.1038/nphoton.2010.214 (https://doi.org/10.1038%2Fnphoton.2010.214). ISSN 1749-4885 (https://search.worldcat.org/issn/1749-4885). S2CID 58897515 (https://api.semanticscholar.org/CorpusID:58897515).
84. Lydersen, Lars; Wiechers, Carlos; Wittmann, Christoffer; Elser, Dominique; Skaar, Johannes; Makarov, Vadim (17 December 2010). "Thermal blinding of gated detectors in quantum cryptography". *Optics Express*. **18** (26): 27938–27954. arXiv:1009.2663 (https://arxiv.org/abs/1009.2663). Bibcode:2010OExpr..1827938L (https://ui.adsabs.harvard.edu/abs/2010OExpr..1827938L). doi:10.1364/oe.18.027938 (https://doi.org/10.1364%2Foe.18.027938). ISSN 1094-4087 (https://search.worldcat.org/issn/1094-4087). PMID 21197067 (https://pubmed.ncbi.nlm.nih.gov/21197067). S2CID 13395490 (https://api.semanticscholar.org/CorpusID:13395490).
85. Wiechers, C; Lydersen, L; Wittmann, C; Elser, D; Skaar, J; Marquardt, Ch; Makarov, V; Leuchs, G (26 January 2011). "After-gate attack on a quantum cryptosystem" (https://doi.org/10.1088%2F1367-2630%2F13%2F1%2F013043). *New Journal of Physics*. **13** (1): 013043. arXiv:1009.2683 (https://arxiv.org/abs/1009.2683). Bibcode:2011NJPh...13a3043W (https://ui.adsabs.harvard.edu/abs/2011NJPh...13a3043W). doi:10.1088/1367-2630/13/1/013043 (https://doi.org/10.1088%2F1367-2630%2F13%2F1%2F013043). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).
86. Jain, Nitin; Wittmann, Christoffer; Lydersen, Lars; Wiechers, Carlos; Elser, Dominique; Marquardt, Christoph; Makarov, Vadim; Leuchs, Gerd (9 September 2011). "Device Calibration Impacts Security of Quantum Key Distribution". *Physical Review Letters*. **107** (11): 110501. arXiv:1103.2327 (https://arxiv.org/abs/1103.2327). Bibcode:2011PhRvL.107k0501J (https://ui.adsabs.harvard.edu/abs/2011PhRvL.107k0501J). doi:10.1103/physrevlett.107.110501 (https://doi.org/10.1103%2Fphysrevlett.107.110501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 22026652 (https://pubmed.ncbi.nlm.nih.gov/22026652). S2CID 6778097 (https://api.semanticscholar.org/CorpusID:6778097).

87. Richard Hughes and Jane Nordholt (16 September 2011). "Refining Quantum Cryptography" (https://zenodo.org/record/1230916). *Science*. **333** (6049): 1584–6. Bibcode:2011Sci...333.1584H (https://ui.adsabs.harvard.edu/abs/2011Sci...333.1584H). doi:10.1126/science.1208527 (https://doi.org/10.1126%2Fscience.1208527). PMID 21921186 (https://pubmed.ncbi.nlm.nih.gov/21921186). S2CID 206535295 (https://api.semanticscholar.org/CorpusID:206535295).
88. Noh, Tae-Gon (1 December 2009). "Counterfactual Quantum Cryptography". *Physical Review Letters*. **103** (23). American Physical Society (APS): 230501. arXiv:0809.3979 (https://arxiv.org/abs/0809.3979). Bibcode:2009PhRvL.103w0501N (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103w0501N). doi:10.1103/physrevlett.103.230501 (https://doi.org/10.1103%2Fphysrevlett.103.230501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 20366133 (https://pubmed.ncbi.nlm.nih.gov/20366133). S2CID 9804265 (https://api.semanticscholar.org/CorpusID:9804265).
89. Thapliyal, Kishore; Pathak, Anirban (26 July 2018). "Kak's three-stage protocol of secure quantum communication revisited: hitherto unknown strengths and weaknesses of the protocol". *Quantum Information Processing*. **17** (9). Springer Science and Business Media LLC: 229. arXiv:1803.02157 (https://arxiv.org/abs/1803.02157). Bibcode:2018QuIP...17..229T (https://ui.adsabs.harvard.edu/abs/2018QuIP...17..229T). doi:10.1007/s11128-018-2001-z (https://doi.org/10.1007%2Fs11128-018-2001-z). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 52009384 (https://api.semanticscholar.org/CorpusID:52009384).
90. "ETSI – Quantum Key Distribution" (http://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution). *etsi.org*. 2014. Retrieved 28 July 2014.
91. "MIQC – European Metrology Research Programme (EMRP)" (http://projects.npl.co.uk/MIQC/index.html). *projects.npl.co.uk*. 2014. Retrieved 28 July 2014.
92. "MIQC2 – European Metrology Research Programme (EMRP)" (http://empir.npl.co.uk/miqc2/). *projects.npl.co.uk*. 2019. Retrieved 18 September 2019.
93. "Quantum Key Distribution" (https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html). *Toshiba*.
94. "CEATEC 2021 ONLINE" (https://web.archive.org/web/20211124205806/https://www.ceatec.com/en/news/infolist_detail.html?id=258). *CEATEC*. Archived from the original (https://www.ceatec.com/en/news/infolist_detail.html?id=258) on 24 November 2021. Retrieved 24 November 2021.
95. "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)" (https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/). National Security Agency. Retrieved 16 July 2022. This article incorporates text from this source, which is in the public domain.
96. Post-Quantum Cryptography: Current state and quantum mitigation, Section 6 "Conclusion" [1] (https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation)
97. "Quantum security technologies" (https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies). *www.ncsc.gov.uk*.
98. "Should Quantum Key Distribution be Used for Secure Communications? | ANSSI" (https://cyber.gouv.fr/en/publications/should-quantum-key-distribution-be-used-secure-communications). *cyber.gouv.fr*.
99. Scarani, Valerio; Kurtsiefer, Christian (4 December 2014). "The black paper of quantum cryptography: Real implementation problems" (https://doi.org/10.1016%2Fj.tcs.2014.09.015). *Theoretical Computer Science*. **560**: 27–32. arXiv:0906.4547 (https://arxiv.org/abs/0906.4547). doi:10.1016/j.tcs.2014.09.015 (https://doi.org/10.1016%2Fj.tcs.2014.09.015). S2CID 44504715 (https://api.semanticscholar.org/CorpusID:44504715).

100. Pacher, Christoph; et, al. (January 2016). "Attacks on quantum key distribution protocols that employ non-ITS authentication" (https://doi.org/10.1007/s11128-015-1160-4). *Quantum Information Processing*. **15** (1): 327–362. arXiv:1209.0365 (https://arxiv.org/abs/1209.0365). Bibcode:2016QuIP...15..327P (https://ui.adsabs.harvard.edu/abs/2016QuIP...15..327P). doi:10.1007/s11128-015-1160-4 (https://doi.org/10.1007%2Fs11128-015-1160-4). S2CID 7779977 (https://api.semanticscholar.org/CorpusID:7779977).
101. Mattsson, J. P.; et al. (December 2021). "Quantum-Resistant Cryptography". arXiv:2112.00399 (https://arxiv.org/abs/2112.00399) [cs.CR (https://arxiv.org/archive/cs.CR)].

External links

General and review

- Quantum Computing 101 (https://web.archive.org/web/20131225083723/https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101)
- Scientific American Magazine (January 2005 Issue) Best-Kept Secrets (https://web.archive.org/web/20071017211849/http://www.sciam.com/article.cfm?chanID=sa006&articleID=000479CD-F58C-11BE-AD0683414B7F0000) Non-technical article on quantum cryptography
- Physics World Magazine (March 2007 Issue) (https://web.archive.org/web/20070704045822/http://physicsweb.org/articles/world/20/3/4/1) Non-technical article on current state and future of quantum communication
- Scarani, Valerio; Bechmann-Pasquinucci, Helle; Cerf, Nicolas J.; Dušek, Miloslav; Lütkenhaus, Norbert; Peev, Momtchil (2009). "The Security of Practical Quantum Key Distribution". *Rev. Mod. Phys*. **81** (3): 1301–1350. arXiv:0802.4155 (https://arxiv.org/abs/0802.4155). Bibcode:2009RvMP...81.1301S (https://ui.adsabs.harvard.edu/abs/2009RvMP...81.1301S). doi:10.1103/RevModPhys.81.1301 (https://doi.org/10.1103%2FRevModPhys.81.1301). S2CID 15873250 (https://api.semanticscholar.org/CorpusID:15873250).
- Nguyen, Kim-Chi; Gilles Van Assche; Cerf, Nicolas J. (2007). "Quantum Cryptography: From Theory to Practice". arXiv:quant-ph/0702202 (https://arxiv.org/abs/quant-ph/0702202).
- SECOQC White Paper on Quantum Key Distribution and Cryptography (https://web.archive.org/web/20160124160241/http://secoqc.net/downloads/secoqc_crypto_wp.pdf) European project to create a large scale quantum cryptography network, includes discussion of current QKD approaches and comparison with classical cryptography
- The future of cryptography (https://web.archive.org/web/20160303183744/http://obfusc.at/ed/cryptography_eng.html) May 2003 Tomasz Grabowski
- ARDA Quantum Cryptography Roadmap (https://web.archive.org/web/20160303180511/http://qist.lanl.gov/qcrypt_map.shtml)
- Lectures at the Institut Henri Poincaré (slides and videos) (https://web.archive.org/web/20160303183533/http://www.quantware.ups-tlse.fr/IHP2006/)
- Interactive quantum cryptography demonstration experiment with single photons for education (https://web.archive.org/web/20121025073450/http://www.didaktik.physik.uni-erlangen.de/quantumlab/english/index.html)

More specific information

- Ekert, Artur (30 April 2005). "Cracking codes, part II | plus.maths.org" (http://pass.maths.org.uk/issue35/features/ekert/index.html). Pass.maths.org.uk. Retrieved 28 December 2013. Description of entanglement based quantum cryptography from Artur Ekert.
- Xu, Qing (2009). *Optical Homodyne Detections and Applications in Quantum Cryptography* (https://tel.archives-ouvertes.fr/pastel-00005580/file/ThesisFull_V2.pdf) (PDF) (Thesis).

Paris: Télécom ParisTech. Retrieved 14 February 2017.
- "Quantum Cryptography and Privacy Amplification" (http://www.ai.sri.com/~goldwate/quantum.html). Ai.sri.com. Retrieved 28 December 2013. Description of BB84 protocol and privacy amplification by Sharon Goldwater.
- Bennett, Charles H.; Brassard, Gilles (2014). "Quantum cryptography: Public key distribution and coin tossing" (https://doi.org/10.1016%2Fj.tcs.2014.05.025). *Theoretical Computer Science*. **560**: 7–11. arXiv:2003.06557 (https://arxiv.org/abs/2003.06557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025).
- Public debate on the Security of Quantum Key Distribution at the conference Hot Topics in Physical Informatics, 11 November 2013 (http://www.ece.tamu.edu/~noise/HotPI_2013/HotPI_2013.html) Archived (https://web.archive.org/web/20160304102648/http://www.ece.tamu.edu/~noise/HotPI_2013/HotPI_2013.html) 4 March 2016 at the Wayback Machine

Further information

- Quantiki.org – Quantum Information portal and wiki (http://www.quantiki.org/)
- Interactive BB84 simulation (http://fredhenle.net/bb84/)

Quantum key distribution simulation

- Online Simulation and Analysis Toolkit for Quantum Key Distribution (https://www.qkdsimulator.com/) Archived (https://web.archive.org/web/20161025035657/https://qkdsimulator.com/) 25 October 2016 at the Wayback Machine

Quantum cryptography research groups

- Experimental Quantum Cryptography with Entangled Photons (https://web.archive.org/web/20050403195032/http://www.quantenkryptographie.at/)
- NIST Quantum Information Networks (https://web.archive.org/web/20070608044014/http://w3.antd.nist.gov/quin.shtml)
- Free Space Quantum Cryptography (http://xqp.physik.uni-muenchen.de/)
- Experimental Continuous Variable QKD, MPL Erlangen (http://www.mpl.mpg.de/index.php?id=125&L=0#QKD)
- Experimental Quantum Hacking, MPL Erlangen (http://www.mpl.mpg.de/index.php?id=125&L=0#QC)
- Quantum cryptography lab. Pljonkin A.P. (https://web.archive.org/web/20170914001740/http://pljonkins.ru/)

Companies selling quantum devices for cryptography

- AUREA Technology (http://aureatechnology.com) sells the optical building blocks for Quantum cryptography
- id Quantique (http://idquantique.com) sells Quantum Key Distribution products
- MagiQ Technologies (http://magiqtech.com) sells quantum devices for cryptography
- QuintessenceLabs (https://web.archive.org/web/20150205054629/http://www.quintessencelabs.com/) Solutions based on continuous wave lasers
- SeQureNet (https://web.archive.org/web/20180406234845/http://www.sequrenet.com/) sells Quantum Key Distribution products using continuous-variables

Companies with quantum cryptography research programmes

- Toshiba (https://web.archive.org/web/20070430232220/http://www.toshiba-europe.com/research/crl/qig/quantumkeyserver.html)
- Hewlett Packard (https://web.archive.org/web/20070303120328/http://www.hpl.hp.com/research/qip/)
- IBM (https://web.archive.org/web/20070607201321/http://www.almaden.ibm.com/st/quantum_information/qcrypt/)
- Mitsubishi (https://web.archive.org/web/20070927094114/http://global.mitsubishielectric.com/bu/security/rd/rd03.html)
- NEC (http://www.nec.co.jp/rd/Eng/Topics/index.html)
- NTT (https://web.archive.org/web/20070205060027/http://www.brl.ntt.co.jp/E/research/qo/qo.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_key_distribution&oldid=1241679323"

WIKIPEDIA
The Free Encyclopedia

BB84

BB84[1][2] is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol.[3] The protocol is provably secure assuming a perfect implementation, relying on two conditions: (1) the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal (see no-cloning theorem); and (2) the existence of an authenticated public classical channel.[4] It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.[5] The proof of BB84 depends on a perfect implementation. Side channel attacks exist, taking advantage of non-quantum sources of information. Since this information is non-quantum, it can be intercepted without measuring or cloning quantum particles.[6]

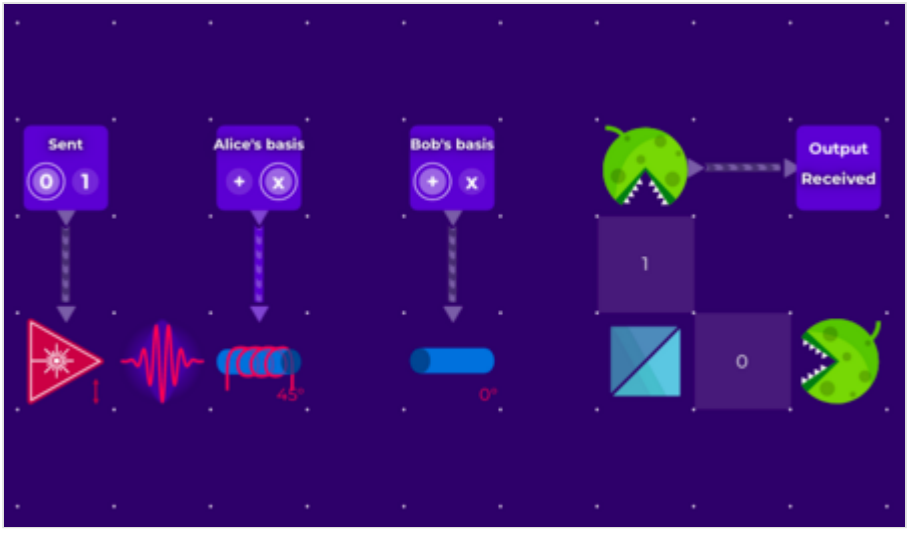
Description

In the BB84 scheme, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a tensor product of n qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle,$$

where a_i and b_i are the i-th bits of a and b respectively. Together, $a_i b_i$ give us an index into the following four qubit states:

$$|\psi_{00}\rangle = |0\rangle,$$
$$|\psi_{10}\rangle = |1\rangle,$$



An interactive simulation of an optical implementation of the BB84 quantum key distribution protocol in the Virtual Lab by Quantum Flytrap,[7] available online (https://lab.quantumflytrap.com/lab/bb84). In this optical setup, bits are encoded using orthogonal polarization states of photons. Alice and Bob select their measurement bases by rotating the polarization by 0 or 45 degrees using Faraday rotators. Single-photon detectors measure the output after the photons pass through a polarizing beam splitter, which separates the polarizations.

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$
$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Note that the bit b_i is what decides which basis a_i is encoded in (either in the computational basis or the Hadamard basis). The qubits are now in states that are not mutually orthogonal, and thus it is impossible to distinguish all of them with certainty without knowing b.

Alice sends $|\psi\rangle$ over a public and authenticated quantum channel $\mathcal{E}$ to Bob. Bob receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ represents both the effects of noise in the channel and eavesdropping by a third party we'll call Eve. After Bob receives the string of qubits, both Bob and Eve have their own states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits. Also, after Bob has received the qubits, we know that Eve cannot be in possession of a copy of the qubits sent to Bob, by the no-cloning theorem, unless she has made measurements. Her measurements, however, risk disturbing a particular qubit with probability $\frac{1}{2}$ if she guesses the wrong basis.

Bob proceeds to generate a string of random bits b' of the same length as b and then measures the qubits he has received from Alice, obtaining a bit string a'. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b, i.e., the bases in which the qubits were prepared. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the bits in a and a' where b and b' do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

See also

- SARG04
- E91 – quantum cryptographic communication protocol

References

1. C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984. http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf Archived (https://web.archive.org/web/20200130165639/http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf) 2020-01-30 at the Wayback Machine
2. Bennett, Charles H.; Brassard, Gilles (2014-12-04). "Quantum cryptography: Public key distribution and coin tossing" (https://doi.org/10.1016%2Fj.tcs.2014.05.025). *Theoretical Computer Science*. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84. 560, Part 1: 7–11. arXiv:2003.06557 (https://arxiv.org/abs/2003.06557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025).
3. Branciard, Cyril; Gisin, Nicolas; Kraus, Barbara; Scarani, Valerio (2005). "Security of two quantum cryptography protocols using the same four qubit states". *Physical Review A*. **72** (3): 032301. arXiv:quant-ph/0505035 (https://arxiv.org/abs/quant-ph/0505035). Bibcode:2005PhRvA..72c2301B (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72c2301

B). doi:10.1103/PhysRevA.72.032301 (https://doi.org/10.1103%2FPhysRevA.72.032301). S2CID 53653084 (https://api.semanticscholar.org/CorpusID:53653084).

4. Scarani, Valerio; Bechmann-Pasquinucci, Helle; Cerf, Nicolas J.; Dušek, Miloslav; Lütkenhaus, Norbert; Peev, Momtchil (2009). "The security of practical quantum key distribution". *Rev. Mod. Phys*. **81** (3): 1301–1350. arXiv:0802.4155 (https://arxiv.org/abs/0802.4155). Bibcode:2009RvMP...81.1301S (https://ui.adsabs.harvard.edu/abs/2009RvMP...81.1301S). doi:10.1103/RevModPhys.81.1301 (https://doi.org/10.1103%2FRevModPhys.81.1301). S2CID 15873250 (https://api.semanticscholar.org/CorpusID:15873250).
5. *Quantum Computing and Quantum Information*, Michael Nielsen and Isaac Chuang, Cambridge University Press 2000
6. Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., Tam, W., Yuan, Z. L., Tanizawa, Y., Sato, H., Kawamura, S., Fujiwara, M., Sasaki, M., & Shields, A. J. (2017). Quantum key distribution with hacking countermeasures and long term field trial. Scientific Reports, 7, 1978.
7. Migdał, Piotr; Jankiewicz, Klementyna; Grabarz, Paweł; Decaroli, Chiara; Cochin, Philippe (2022). "Visualizing quantum mechanics in an interactive simulation - Virtual Lab by Quantum Flytrap". *Optical Engineering*. **61** (8): 081808. arXiv:2203.13300 (https://arxiv.org/abs/2203.13300). doi:10.1117/1.OE.61.8.081808 (https://doi.org/10.1117%2F1.OE.61.8.081808).

Retrieved from "https://en.wikipedia.org/w/index.php?title=BB84&oldid=1221147001"

WIKIPEDIA
The Free Encyclopedia

SARG04

SARG04 (named after Valerio Scarani, Antonio Acín, Gregoire Ribordy, and Nicolas Gisin) is a 2004 quantum cryptography protocol derived from the first protocol of that kind, BB84.

Origin

Researchers built SARG04 when they noticed that by using the four states of BB84 with a different information encoding they could develop a new protocol which would be more robust, especially against the photon-number-splitting attack, when attenuated laser pulses are used instead of single-photon sources. SARG04 was defined by Scarani et al. in 2004 in Physical Review Letters as a prepare and measure version (in which it is equivalent to BB84 when viewed at the level of quantum processing).[1]

An entanglement-based version has been defined as well.[1]

Description

In the SARG04 scheme, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a string of n qubits,

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle.$$

a_i and b_i are the i^{th} bits of a and b, respectively. Together, $a_i b_i$ give us an index into the following four qubit states:

$$|\psi_{00}\rangle = |0\rangle$$

$$|\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Note that the bit b_i is what decides which basis a_i is encoded in (either in the computational basis or the Hadamard basis). The qubits are now in states which are not mutually orthogonal, and thus it is impossible to distinguish all of them with certainty without knowing b.

Alice sends $|\psi\rangle$ over a public quantum channel to Bob. Bob receives a state $\varepsilon\rho = \varepsilon|\psi\rangle\langle\psi|$, where ε represents the effects of noise in the channel as well as eavesdropping by a third party we'll call Eve. After Bob receives the string of qubits, all three parties, namely Alice, Bob and Eve, have their own

states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits.

Bob proceeds to generate a string of random bits b' of the same length as b, and uses those bits for his choice of basis when measuring the qubits transmitted by Alice. At this point, Bob announces publicly that he has received Alice's transmission. For each qubit sent, Alice chooses one computational basis state and one Hadamard basis state such that the state of the qubit is one of these two states. Alice then announces those two states. Alice will note whether the state is the computational basis state or the Hadamard basis state; that piece of information makes up the secret bit that Alice wishes to communicate to Bob. Bob now knows that the state of his qubit was one of the two states indicated by Alice. To determine the secret bit, Bob must distinguish between the two candidate states. For each qubit, Bob can check to see whether his measurement is consistent with either possible state. If it is consistent with either state, Bob announces that the bit is invalid, since he cannot distinguish which state was transmitted based on the measurement. If on the other hand, one of the two candidate states was inconsistent with the observed measurement, Bob announces that the bit is valid since he can deduce the state (and therefore the secret bit).

Consider for example the scenario that Alice transmits $|\psi_{00}\rangle$ and announces the two states $|\psi_{00}\rangle$ and $|\psi_{01}\rangle$. If Bob measures in the computational basis, his only possible measurement is $|\psi_{00}\rangle$. This outcome is clearly consistent with the state having been $|\psi_{00}\rangle$, but it would also be a possible outcome if the state had been $|\psi_{01}\rangle$. If Bob measures in the Hadamard basis, either $|\psi_{01}\rangle$ or $|\psi_{11}\rangle$ could be measured, each with probability $\frac{1}{2}$. If the outcome is $|\psi_{01}\rangle$ then again this state is consistent with either starting state. On the other hand, an outcome of $|\psi_{11}\rangle$ cannot possibly be observed from a qubit in state $|\psi_{01}\rangle$. Thus in the case that Bob measures in the Hadamard basis and observes state $|\psi_{11}\rangle$ (and only in that case), Bob can deduce which state he was sent and therefore what the secret bit is.

From the remaining k bits where both Bob's measurement was conclusive, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see if more than a certain number of them agree. If this check passes, Alice and Bob proceed to use privacy amplification and information reconciliation techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

The advantage of this scheme relative to the simpler BB84 protocol is that Alice never announces the basis of her bit. As a result, Eve needs to store more copies of the qubit in order to be able to eventually determine the state than she would if the basis were directly announced.

Intended use

The intended use of SARG04 is in situations where the information is originated by a Poissonian source producing weak pulses (this means: mean number of photons < 1) and received by an imperfect detector, which is when attenuated laser pulses are used instead of single photons. Such a SARG04 system can be reliable up to a distance of about 10 km.[1]

Modus operandi

The modus operandi of SARG04 is based on the principle that the hardware must remain the same (as prior protocols) and the only change must be in the protocol itself.[1]

In the original "prepare and measure" version, SARG04's two conjugated bases are chosen with equal probability.[1]

Double clicks (when both detectors click) are important for comprehending SARG04: double clicks work differently in BB84 and SARG04. In BB84, their item is discarded because there is no way to tell what bit Alice has sent. In SARG04, they are also discarded, "for simplicity", but their occurrence is monitored to prevent eavesdropping. See the paper for a full quantum analysis of the various cases.[1]

Security

Kiyoshi Tamaki and Hoi-Kwong Lo were successful in proving security for one and two-photon pulses using SARG04.[1]

It has been confirmed that SARG04 is more robust than BB84 against incoherent PNS attacks.[1]

Unfortunately an incoherent attack has been identified which performs better than a simple phase-covariant cloning machine, and SARG04 has been found to be particularly vulnerable in single-photon implementations when Q >= 14.9%.[1]

Comparison with BB84

In single-photon implementations, SARG04 was theorised to be equal with BB84, but experiments have shown that it is inferior.[1]

References

1. Cyril Branciard; Nicolas Gisin; Barbara Kraus; Valerio Scarani (2005). "Security of two quantum cryptography protocols using the same four qubit states". *Physical Review A*. **72** (3): 032301. arXiv:quant-ph/0505035 (https://arxiv.org/abs/quant-ph/0505035). Bibcode:2005PhRvA..72c2301B (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72c2301B). doi:10.1103/PhysRevA.72.032301 (https://doi.org/10.1103%2FPhysRevA.72.032301).

Bibliography

- Valerio Scarani; Antonio Acín; Grégoire Ribordy; Nicolas Gisin (2004). "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". *Physical Review Letters*. **92** (5): 057901. arXiv:quant-ph/0211131 (https://arxiv.org/abs/quant-ph/0211131). Bibcode:2004PhRvL..92e7901S (https://ui.adsabs.harvard.edu/abs/2004PhRvL..92e7901S). doi:10.1103/PhysRevLett.92.057901 (https://doi.org/10.1103%2FPhysRevLett.92.057901). PMID 14995344 (https://pubmed.ncbi.nlm.nih.gov/14995344).
- Chi-Hang Fred Fung; Kiyoshi Tamaki; Hoi-Kwong Lo (2006). "Performance of two quantum-key-distribution protocols". *Physical Review A*. **73** (1): 012337. arXiv:quant-ph/0510025 (http

s://arxiv.org/abs/quant-ph/0510025). Bibcode:2006PhRvA..73a2337F (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73a2337F). doi:10.1103/PhysRevA.73.012337 (https://doi.org/10.1103%2FPhysRevA.73.012337).

- Branciard, Cyril; Gisin, Nicolas; Kraus, Barbara; Scarani, Valerio (2005). "Security of two quantum cryptography protocols using the same four qubit states". *Physical Review A*. **72**: 32301. arXiv:quant-ph/0505035 (https://arxiv.org/abs/quant-ph/0505035). Bibcode:2005PhRvA..72c2301B (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72c2301B). doi:10.1103/physreva.72.032301 (https://doi.org/10.1103%2Fphysreva.72.032301).

See also

- Quantum cryptography
- BB84 protocol

Retrieved from "https://en.wikipedia.org/w/index.php?title=SARG04&oldid=1230115053"

WIKIPEDIA
The Free Encyclopedia

List of quantum key distribution protocols

Quantum key distribution (QKD) protocols are used in quantum key distribution. The first protocol of that kind was BB84, introduced in 1984 by Charles H. Bennett and Gilles Brassard. After that, many other protocols have been defined.

List of quantum key distribution protocols

- BB84 (1984) is a quantum key distribution scheme that allows two parties to securely communicate a private key for use in one-time pad encryption using the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal and an authenticated public classical channel.[1]
- E91 protocol (1991) is a quantum cryptography method that uses entangled pairs of photons to generate keys for secure communication, with the ability to detect any attempts at eavesdropping by an external party through the violation of Bell's Theorem and the preservation of perfect correlation between the measurements of the two parties.
- BBM92 protocol (1992) is a quantum key distribution method that uses polarized entangled photon pairs and decoy states to securely transmit non-orthogonal quantum signals.
- B92 protocol (1992) is a quantum key distribution method that uses entanglement distillation protocols to prepare and transmit nonorthogonal quantum states with unconditional security, even over lossy and noisy channels, by measuring the state on the Z basis and using local filtering and Z basis measurements to ensure the security of the transmission is determined by the number of errors and the number of filter pairs used.
- MSZ96 protocol (1996) uses four nonorthogonal quantum states of a weak optical field to encode a cryptographic key bit without the use of photon polarization or entangled photons.
- Six-state protocol (1998) is a method of transmitting secure information using quantum cryptography that is more resistant to noise and easier to detect errors in compared to the BB84 protocol, due to its use of a six-state polarization scheme on three orthogonal bases and its ability to tolerate a noisier channel.
- DPS protocol (2002) is a simple and efficient quantum key distribution (QKD) method that does not require a basis selection process like the traditional BB84 protocol, has a simpler receiver configuration with fewer detectors, uses efficient sequential pulses in the time domain for high key creation speed, and is robust against photon-number splitting attacks even with weak coherent light.
- Decoy state protocol (2003) is a method used in practical quantum cryptography systems that uses multiple intensity levels at the transmitter's source and monitors bit error rates to detect and prevent photon number splitting attacks, enabling higher secure transmission rates or longer maximum channel lengths.
- SARG04 (2004) is a quantum key distribution protocol that was developed as a more robust version of BB84, especially against photon-number-splitting attacks, for use with attenuated laser pulses in situations where the information is originated by a Poissonian source producing weak pulses and received by an imperfect detector.
- COW protocol (2005) allows for secure communication between two parties by transmitting a key using weak coherent pulses of light and has advantages of requiring only a random

number generator on the client side and being able to transmit key information at a high rate.

- Three-stage quantum cryptography protocol (2006) is a method of data encryption that uses random polarization rotations by the two authenticated parties, to continuously encrypt data using single photons and can also be used for exchanging keys, with the possibility of multi-photon quantum cryptography and the ability to address man-in-the-middle attacks through modification.
- KMB09 protocol (2009) allows for increased transmission distances between Alice and Bob by using two mutually unbiased bases and introducing a minimum index transmission error rate and quantum bit error rate, which is particularly effective for higher-dimensional photon states.
- HDQKD is a technology that enables secure communication between two parties by encoding quantum information in high dimensions, such as optical angular momentum modes, and transmitting it over long distances through multicore fibers or free-space links.
- T12 protocol aims to increase the practicality of QKD by removing certain idealizations and including features that can increase the key rate of the system.

References

1. Sabani, Maria; Savvas, Ilias; Poulakis, Dimitrios; Makris, Georgios (2022). "Quantum Key Distribution: Basic Protocols and Threats". *Proceedings of the 26th Pan-Hellenic Conference on Informatics*. pp. 383–388. doi:10.1145/3575879.3576022 (https://doi.org/10.1145%2F3575879.3576022). ISBN 978-1-4503-9854-1.

Retrieved from "https://en.wikipedia.org/w/index.php?title=List_of_quantum_key_distribution_protocols&oldid=1240914338"

WIKIPEDIA
The Free Encyclopedia

Quantum secret sharing

Quantum secret sharing (**QSS**) is a quantum cryptographic scheme for secure communication that extends beyond simple quantum key distribution. It modifies the classical secret sharing (CSS) scheme by using quantum information and the no-cloning theorem to attain the ultimate security for communications.

The method of secret sharing consists of a sender who wishes to share a secret with a number of receiver parties in such a way that the secret is fully revealed only if a large enough portion of the receivers work together. However, if not enough receivers work together to reveal the secret, the secret remains completely unknown.

The classical scheme was independently proposed by Adi Shamir[1] and George Blakley[2] in 1979. In 1998, Mark Hillery, Vladimír Bužek, and André Berthiaume extended the theory to make use of quantum states for establishing a secure key that could be used to transmit the secret via classical data.[3] In the years following, more work was done to extend the theory to transmitting quantum information as the secret, rather than just using quantum states for establishing the cryptographic key.[4][5]

QSS has been proposed for being used in quantum money[6] as well as for joint checking accounts, quantum networking, and distributed quantum computing, among other applications.

Protocol

The simplest case: GHZ states

This example follows the original scheme laid out by Hillery et al. in 1998 which makes use of Greenberger–Horne–Zeilinger (GHZ) states. A similar scheme was developed shortly thereafter which used two-particle entangled states instead of three-particle states.[7] In both cases, the protocol is essentially an extension of quantum key distribution to two receivers instead of just one.

Following the typical language, let the sender be denoted as Alice and two receivers as Bob and Charlie. Alice's objective is to send each receiver a "share" of her secret key (really just a quantum state) in such a way that:

1. Neither Bob's nor Charlie's share contains any information about Alice's original message, and therefore neither can extract the secret on their own.
2. The secret can only be extracted if Bob and Charlie work together, in which case the secret is fully revealed.
3. The presence of either an outside eavesdropper or a dishonest receiver (either Bob or Charlie) can be detected without the secret being revealed.

Alice initiates the protocol by sharing with each of Bob and Charlie one particle from a GHZ triplet in the (standard) Z-basis, holding onto the third particle herself:

$$|\Psi\rangle_{\mathbf{GHZ}} = \frac{|000\rangle + |111\rangle}{\sqrt{2}},$$

where $|0\rangle$ and $|1\rangle$ are orthogonal modes in an arbitrary Hilbert space.

After each participant measures their particle in the X- or Y-basis (chosen at random), they share (via a classical, public channel) which basis they used to make the measurement, but not the result itself. Upon combining their measurement results, Bob and Charlie can deduce what Alice measured 50% of the time. Repeating this process many times, and using a small fraction to verify that no malicious actors are present, the three participants can establish a joint key for communicating securely. Consider the following for a clear example of how this will work.

Let us define the x and y eigenstates in the following, standard way:

$$|+\mathbf{x}\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |-\mathbf{x}\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$
$$|+\mathbf{y}\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, |-\mathbf{y}\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}.$$

The GHZ state can then be rewritten as

$$|\Psi\rangle_{\mathbf{GHZ}} = \frac{1}{2\sqrt{2}}[(|+x\rangle_a|+x\rangle_b + |-x\rangle_a|-x\rangle_b)(|0\rangle_c + |1\rangle_c) + (|+x\rangle_a|-x\rangle_b + |-x\rangle_a|+x\rangle_b)(|0\rangle_c - |1\rangle_c)]$$

,

where (a, b, c) denote the particles for (Alice, Bob, Charlie) and Alice's and Bob's states have been written in the X-basis. Using this form, it is evident that their exists a correlation between Alice's and Bob's measurements and Charlie's single-particle state:

if Alice and Bob have correlated results then Charlie has the state $\frac{|0\rangle_c + |1\rangle_c}{\sqrt{2}}$ and if Alice and Bob have anticorrelated results then Charlie has the state $\frac{|0\rangle_c - |1\rangle_c}{\sqrt{2}}$.

It is clear from the table summarizing these correlations that by knowing the measurement bases of Alice and Bob, Charlie can use his own measurement result to deduce whether Alice and Bob had the same or opposite results. Note however that to make this deduction, Charlie must choose the correct measurement basis for measuring his own particle. Since he chooses between two noncommuting bases at random, only half of the time will he be able to extract useful information. The other half of the time the results must be discarded. Additionally, from the table one can see that Charlie has no way of determining who measured what, only if the results of Alice and Bob were correlated or anticorrelated. Thus the only way for Charlie to figure out Alice's measurement is by working together with Bob and sharing their results. In doing so, they can extract Alice's results for every measurement and use this information to create a cryptographic key that only they know.

		Alice			
		+x	-x	+y	-y
Bob	+x	|0⟩ + |1⟩	|0⟩ − |1⟩	|0⟩ − i|1⟩	|0⟩ + i|1⟩
	-x	|0⟩ − |1⟩	|0⟩ + |1⟩	|0⟩ + i|1⟩	|0⟩ − i|1⟩
	+y	|0⟩ − i|1⟩	|0⟩ + i|1⟩	|0⟩ − |1⟩	|0⟩ + |1⟩
	-y	|0⟩ + i|1⟩	|0⟩ − i|1⟩	|0⟩ + |1⟩	|0⟩ − |1⟩

The effect of Alice's and Bob's measurements on Charlie's state for the standard GHZ triplet.

((*k*,*n*)) threshold scheme

The simple case described above can be extended similarly to that done in CSS by Shamir and Blakley via a thresholding scheme. In the $((k,n))$ threshold scheme (double parentheses denoting a quantum scheme), Alice splits her secret key (quantum state) into n shares such that any k≤n shares are required to extract the full information but k-1 or less shares cannot extract *any* information about Alice's key.

The number of users needed to extract the secret is bounded by $n/2 < k \leq n$. Consider for $n \geq 2k$, if a $((k,n))$ threshold scheme is applied to two disjoint sets of *k* in *n*, then two independent copies of Alice's secret can be reconstructed. This of course would violate the no-cloning theorem and is why n must be less than 2k.

As long as a $((k,n))$ threshold scheme exists, a $((k,n\text{-}1))$ threshold scheme can be constructed by simply discarding one share. This method can be repeated until k=n.

The following outlines a simple ((2,3)) threshold scheme,[4] and more complicated schemes can be imagined by increasing the number of shares Alice splits her original state into:

Consider Alice beginning with the single qutrit state

$$|\Psi\rangle_a = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle,$$

and then mapping it to three qutrits

$$|\psi\rangle = \alpha(|000\rangle + |111\rangle + |222\rangle) + \beta(|012\rangle + |120\rangle + |201\rangle) + \gamma(|021\rangle + |102\rangle + |210\rangle)$$

and sharing one qutrit with each of the 3 receivers. It is evident that a single share does not give any information about Alice's original state, since each share is in the maximally mixed state. However, two shares could be used to reconstruct Alice's original state. Assume the first two shares are given. Add the first share to the second (modulo three) and then add the new value of the second share to the first. The resulting state is

$$|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)(|00\rangle + |12\rangle + |21\rangle)$$

where the first qutrit is exactly Alice's original state. Via this method, the sender's original state can be reconstructed at one of the receivers' particles, but it is crucial that no measurements be made during this reconstruction process or any superposition within the quantum state will collapse.

Security

The security of QSS relies upon the no-cloning theorem to protect against possible eavesdroppers as well as dishonest users. This section adopts the two-particle entanglement protocol very briefly mentioned above.[7]

Eavesdropping

QSS promises security against eavesdropping in the exact same way as quantum key distribution. Consider an eavesdropper, Eve, who is assumed to be capable of perfectly discriminating and creating the quantum states used in the QSS protocol. Eve's objective is to intercept one of the receivers' (say Bob's) shares, measure it, then recreate the state and send it on to whomever the share was initially intended for. The issue with this method is that Eve needs to randomly choose a basis to measure in, and half of the time she will choose the wrong basis. When she chooses the correct basis, she will get the correct measurement result with certainty and can recreate the state she measured and send it off to Bob without her presence being detected. However, when she chooses the wrong basis, she will end up sending one of the two states from the incorrect basis. Bob will measure the state she sent him and half of the time this will be the correct detection, but only because the state from the wrong basis is an equal superposition of the two states in the correct basis. Thus, half of the time that Eve measures in the wrong basis and therefore sends the incorrect state, Bob will measure the wrong state. This intervention on Eve's part leads to causing an error in the protocol on an extra 25% of trials. Therefore, with enough measurements, it will be nearly impossible to miss the protocol errors occurring with a 75% probability instead of the 50% probability predicted by the theory, thus signaling that there is an eavesdropper within the communication channel.

More complex eavesdropping strategies can be performed using ancilla states, but the eavesdropper will still be detectable in a similar manner.

Dishonest participant

Now, consider the case where one of the participants of the protocol (say Bob) is acting as a malicious user by trying to obtain the secret without the other participants being aware. Analyzing the possibilities, one learns that choosing the proper order in which Bob and Charlie release their measurement bases and results *when testing for eavesdropping* can promise the detection of any cheating that may be occurring. The proper order turns out to be:

1. Receiver 1 releases measurement results.
2. Receiver 2 releases measurement results.
3. Receiver 2 releases measurement basis.
4. Receiver 1 releases measurement basis.

This ordering prevents receiver 2 from knowing which basis to share for tricking the other participants because receiver 2 does not yet know what basis receiver 1 is going to announce was used. Similarly, since receiver 1 must release their results first, they cannot control if the measurements should be correlated or anticorrelated for the valid combination of bases used. In this way, acting dishonestly will introduce errors in the eavesdropper testing phase whether the dishonest participant is receiver 1 or receiver 2. Thus, the ordering of releasing the data must be carefully chosen so as to prevent any dishonest user from acquiring the secret without being noticed by the other participants.

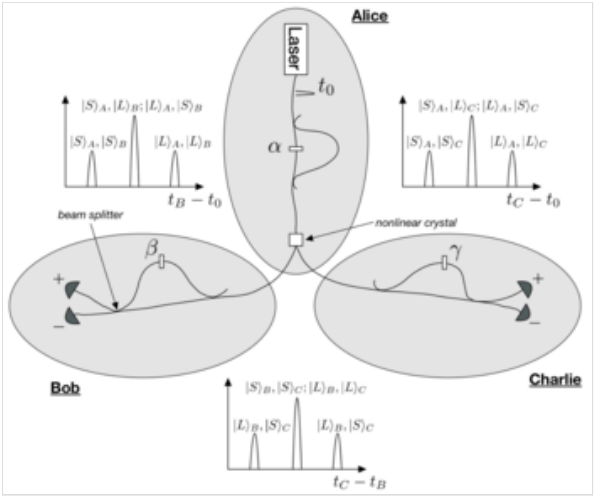
Experimental realization

This section follows from the first experimental demonstration of QSS in 2001 which was made possible via advances in techniques of quantum optics.[8]

The original idea for QSS using GHZ states was more challenging to implement because of the difficulties in producing three-particle correlations via either down-conversion processes with χ^3 nonlinearities or three-photon positronium annihilation, both of which are rare events.[9] Instead, the original experiment was performed via the two-particle scheme using a standard χ^2 spontaneous parametric down-conversion (SPDC) process with the third correlated photon being the pump photon.

The experimental setup works as follows:

- Alice: A pulsed laser emitted at time t_0 enters an interferometer with unequal path lengths such that the pump is split into two distinct temporal pulses with equal amplitude. One arm of the interferometer contains a phase shifter to control the phase difference of the two arms, denoted α. The pump pulses are focused onto a nonlinear crystal where some of the pump photons are down-converted into photon pairs via SPDC. The SPDC pairs are then split, with one being sent to Bob and the other to Charlie.
- Bob and Charlie: Both receivers have identical interferometers to the one used by Alice such that the exact same time difference between the two arms is achieved and each has a phase shifter denoted as β for Bob and γ for Charlie. The different possible trajectories of each interferometer lead to three distinct time differences between when Alice's pump pulse is emitted and when Bob's and Charlie's SPDC photons are detected (t_B and t_C, respectively), as well as three time differences between the detections at each of Bob's and Charlie's detectors.



Two-photon quantum secret sharing (QSS) setup via spontaneous parametric down-conversion (SPDC)

Using $|\mathbf{X}\rangle_i, |\mathbf{Y}\rangle_j$ where X and Y are either 'S' for short path or 'L' for long path and i and j are one of 'A', 'B', or 'C' to label a participant's interferometer, this notation describes the arbitrary path taken for any combination of two participants. Notice that $|\mathbf{S}\rangle_A, |\mathbf{L}\rangle_j$ and $|\mathbf{L}\rangle_A, |\mathbf{S}\rangle_j$ where j is either 'B' or 'C' are indistinguishable processes as the time difference between the two processes are exactly the same. The same is true for $|\mathbf{S}\rangle_B, |\mathbf{S}\rangle_C$ and $|\mathbf{L}\rangle_B, |\mathbf{L}\rangle_C$. Describing these indistinguishable processes mathematically,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|L\rangle_A, |S\rangle_B|S\rangle_C + e^{i(\alpha+\beta+\gamma)}|S\rangle_A, |L\rangle_B|L\rangle_C)),$$

which can be thought of as a "pseudo-GHZ state" where the difference from a true GHZ state is that the three photons do not exist simultaneously. Nonetheless, the triple "coincidences" can be described by exactly the same probability function as for the true GHZ state,

$$P_{i,j,k} = \frac{1}{8}(1 + ijk\cos(\alpha+\beta+\gamma)),$$

implying that QSS will work just the same for this 2-particle source.

By setting the phases $\alpha, \beta,$ and γ to either 0 or $\frac{\pi}{2}$ in much the same way as two-photon Bell tests, it can be shown that this setup violates a Bell-type inequality for three particles,

$$S_3 = |E(\alpha'+\beta+\gamma) + E(\alpha+\beta'+\gamma) + E(\alpha+\beta+\gamma') - E(\alpha'+\beta'+\gamma')| \leq 2,$$

where $E(\alpha+\beta+\gamma)$ is the expectation value for a coincidence measurement with phase shifter settings (α, β, γ). For this experiment, the Bell-type inequality was violated, with $S_{\text{exp}} = 3.69$, suggesting that this setup exhibits quantum nonlocality.

This seminal experiment showed that the quantum correlations from this setup are indeed described by the probability function $P_{i,j,k}$. The simplicity of the SPDC source allowed for coincidences at much higher rates than traditional three-photon entanglement sources, making QSS more practical. This was the first experiment to prove the feasibility of a QSS protocol.

References

1. Shamir, Adi (1 November 1979). "How to share a secret" (https://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf) (PDF). *Communications of the ACM*. **22** (11): 612–613. doi:10.1145/359168.359176 (https://doi.org/10.1145%2F359168.359176). S2CID 16321225 (https://api.semanticscholar.org/CorpusID:16321225). Archived (https://web.archive.org/web/20170810232803/http://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf) (PDF) from the original on 2017-08-10.
2. Blakley, G.R. (1979). "Safeguarding Cryptographic Keys" (https://web.archive.org/web/20180628164048/https://pdfs.semanticscholar.org/32d2/1ccc21a807627fcb21ea829d1acdab23be12.pdf) (PDF). *Managing Requirements Knowledge, International Workshop on (AFIPS)*. **48**: 313–317. doi:10.1109/AFIPS.1979.98 (https://doi.org/10.1109%2FAFIPS.1979.98). S2CID 38199738 (https://api.semanticscholar.org/CorpusID:38199738). Archived from the original (https://pdfs.semanticscholar.org/32d2/1ccc21a807627fcb21ea829d1acdab23be12.pdf) (PDF) on 2018-06-28.
3. Hillery, Mark; Bužek, Vladimír; Berthiaume, André (1998). "Quantum Secret Sharing". *Physical Review A*. **59** (3): 1829–1834. arXiv:quant-ph/9806063 (https://arxiv.org/abs/quant-ph/9806063). doi:10.1103/PhysRevA.59.1829 (https://doi.org/10.1103%2FPhysRevA.59.1829). S2CID 55165469 (https://api.semanticscholar.org/CorpusID:55165469).
4. Cleve, Richard; Gottesman, Daniel; Lo, Hoi-Kwong (1999). "How to share a quantum secret". *Physical Review Letters*. **83** (3): 648–651. arXiv:quant-ph/9901025 (https://arxiv.org/abs/quant-ph/9901025). Bibcode:1999PhRvL..83..648C (https://ui.adsabs.harvard.edu/abs/1999PhRvL..83..648C). doi:10.1103/PhysRevLett.83.648 (https://doi.org/10.1103%2FPhysRevLett.83.648). S2CID 7397021 (https://api.semanticscholar.org/CorpusID:7397021).
5. Gottesman, Daniel (2000). "Theory of quantum secret sharing" (https://journals.aps.org/pra/pdf/10.1103/PhysRevA.61.042311). *Physical Review A*. **61** (4): 042311. arXiv:quant-ph/9910067 (https://arxiv.org/abs/quant-ph/9910067). Bibcode:2000PhRvA..61d2311G (https://ui.adsabs.harvard.edu/abs/2000PhRvA..61d2311G). doi:10.1103/PhysRevA.61.042311 (https://doi.org/10.1103%2FPhysRevA.61.042311). S2CID 45581685 (https://api.semanticscholar.org/CorpusID:45581685). Retrieved 14 December 2021.
6. Wiesner, Stephen (January 1983). "Conjugate coding". *ACM SIGACT News*. **15** (1): 78–88. doi:10.1145/1008908.1008920 (https://doi.org/10.1145%2F1008908.1008920). S2CID 207155055 (https://api.semanticscholar.org/CorpusID:207155055).
7. Karlsson, Anders; Koashi, Masato; Imoto, Nobuyuki (1999). "Quantum entanglement for secret sharing and secret splitting" (https://journals.aps.org/pra/pdf/10.1103/PhysRevA.59.162). *Physical Review A*. **59** (1): 162–168. Bibcode:1999PhRvA..59..162K (https://ui.adsabs.harvard.edu/abs/1999PhRvA..59..162K). doi:10.1103/PhysRevA.59.162 (https://doi.org/10.1103%2FPhysRevA.59.162). Retrieved 14 December 2021.
8. Tittel, W.; Zbinden, H.; Gisin, N. (2001). "Experimental demonstration of quantum secret sharing" (https://journals.aps.org/pra/pdf/10.1103/PhysRevA.63.042301). *Physical Review A*. **63** (4): 042301. Bibcode:2001PhRvA..63d2301T (https://ui.adsabs.harvard.edu/abs/2001PhRvA..63d2301T). doi:10.1103/PhysRevA.63.042301 (https://doi.org/10.1103%2FPhysRevA.63.042301). Retrieved 15 December 2021.
9. Żukowski, M.; Zeilinger, A.; Horne, M.A.; Weinfurter, H. (1998). "Quest for GHZ states" (http://przyrbwn.icm.edu.pl/APP/PDF/93/a093z1p15.pdf) (PDF). *Acta Physica Polonica A*. **98** (1): 187–195. Bibcode:1998AcPPA..93..187Z (https://ui.adsabs.harvard.edu/abs/1998AcPPA..93..187Z). doi:10.12693/APhysPolA.93.187 (https://doi.org/10.12693%2FAPhysPolA.93.187). Retrieved 15 December 2021.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_secret_sharing&oldid=1192020889"

WIKIPEDIA
The Free Encyclopedia

Quantum algorithm

In quantum computing, a **quantum algorithm** is an algorithm that runs on a realistic model of quantum computation, the most commonly used model being the quantum circuit model of computation.[1][2] A classical (or non-quantum) algorithm is a finite sequence of instructions, or a step-by-step procedure for solving a problem, where each step or instruction can be performed on a classical computer. Similarly, a quantum algorithm is a step-by-step procedure, where each of the steps can be performed on a quantum computer. Although all classical algorithms can also be performed on a quantum computer,[3]:126 the term quantum algorithm is generally reserved for algorithms that seem inherently quantum, or use some essential feature of quantum computation such as quantum superposition or quantum entanglement.

Problems that are undecidable using classical computers remain undecidable using quantum computers.[4]:127 What makes quantum algorithms interesting is that they might be able to solve some problems faster than classical algorithms because the quantum superposition and quantum entanglement that quantum algorithms exploit generally cannot be efficiently simulated on classical computers (see Quantum supremacy).

The best-known algorithms are Shor's algorithm for factoring and Grover's algorithm for searching an unstructured database or an unordered list. Shor's algorithm runs much (almost exponentially) faster than the best-known classical algorithm for factoring, the general number field sieve.[5] Grover's algorithm runs quadratically faster than the best possible classical algorithm for the same task,[6] a linear search.

Overview

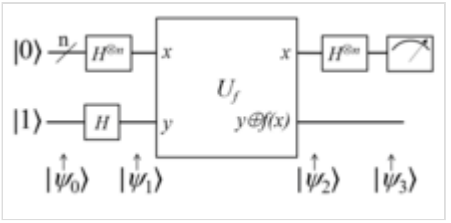
Quantum algorithms are usually described, in the commonly used circuit model of quantum computation, by a quantum circuit that acts on some input qubits and terminates with a measurement. A quantum circuit consists of simple quantum gates, each of which acts on some finite number of qubits. Quantum algorithms may also be stated in other models of quantum computation, such as the Hamiltonian oracle model.[7]

Quantum algorithms can be categorized by the main techniques involved in the algorithm. Some commonly used techniques/ideas in quantum algorithms include phase kick-back, phase estimation, the quantum Fourier transform, quantum walks, amplitude amplification and topological quantum field theory. Quantum algorithms may also be grouped by the type of problem solved; see, e.g., the survey on quantum algorithms for algebraic problems.[8]

Algorithms based on the quantum Fourier transform

The quantum Fourier transform is the quantum analogue of the discrete Fourier transform, and is used in several quantum algorithms. The Hadamard transform is also an example of a quantum Fourier transform over an n-dimensional vector space over the field $\mathbf{F}_2$. The quantum Fourier transform can be efficiently implemented on a quantum computer using only a polynomial number of quantum gates.

Deutsch–Jozsa algorithm



Deutsch-Jozsa algorithm

The Deutsch–Jozsa algorithm solves a black-box problem that requires exponentially many queries to the black box for any deterministic classical computer, but can be done with a single query by a quantum computer. However, when comparing bounded-error classical and quantum algorithms, there is no speedup, since a classical probabilistic algorithm can solve the problem with a constant number of queries with small probability of error. The algorithm determines whether a function f is either constant (0 on all inputs or 1 on all inputs) or balanced (returns 1 for half of the input domain and 0 for the other half).

Bernstein–Vazirani algorithm

The Bernstein–Vazirani algorithm is the first quantum algorithm that solves a problem more efficiently than the best known classical algorithm. It was designed to create an oracle separation between BQP and BPP.

Simon's algorithm

Simon's algorithm solves a black-box problem exponentially faster than any classical algorithm, including bounded-error probabilistic algorithms. This algorithm, which achieves an exponential speedup over all classical algorithms that we consider efficient, was the motivation for Shor's algorithm for factoring.

Quantum phase estimation algorithm

The quantum phase estimation algorithm is used to determine the eigenphase of an eigenvector of a unitary gate, given a quantum state proportional to the eigenvector and access to the gate. The algorithm is frequently used as a subroutine in other algorithms.

Shor's algorithm

Shor's algorithm solves the discrete logarithm problem and the integer factorization problem in polynomial time,[9] whereas the best known classical algorithms take super-polynomial time. These problems are not known to be in P or NP-complete. It is also one of the few quantum algorithms that solves a non–black-box problem in polynomial time, where the best known classical algorithms run in super-polynomial time.

Hidden subgroup problem

The abelian hidden subgroup problem is a generalization of many problems that can be solved by a quantum computer, such as Simon's problem, solving Pell's equation, testing the principal ideal of a ring R and factoring. There are efficient quantum algorithms known for the Abelian hidden subgroup problem.[10] The more general hidden subgroup problem, where the group isn't necessarily abelian, is a generalization of the previously mentioned problems, as well as graph isomorphism and certain lattice problems. Efficient quantum algorithms are known for certain non-abelian groups. However, no efficient algorithms are known for the symmetric group, which would give an efficient algorithm for graph isomorphism[11] and the dihedral group, which would solve certain lattice problems.[12]

Estimating Gauss sums

A Gauss sum is a type of exponential sum. The best known classical algorithm for estimating these sums takes exponential time. Since the discrete logarithm problem reduces to Gauss sum estimation, an efficient classical algorithm for estimating Gauss sums would imply an efficient classical algorithm for computing discrete logarithms, which is considered unlikely. However, quantum computers can estimate Gauss sums to polynomial precision in polynomial time.[13]

Fourier fishing and Fourier checking

Consider an oracle consisting of n random Boolean functions mapping n-bit strings to a Boolean value, with the goal of finding n n-bit strings $z_1,...,z_n$ such that for the Hadamard-Fourier transform, at least 3/4 of the strings satisfy

$$|\tilde{f}(z_i)| \geqslant 1$$

and at least 1/4 satisfy

$$|\tilde{f}(z_i)| \geqslant 2.$$

This can be done in bounded-error quantum polynomial time (BQP).[14]

Algorithms based on amplitude amplification

Amplitude amplification is a technique that allows the amplification of a chosen subspace of a quantum state. Applications of amplitude amplification usually lead to quadratic speedups over the corresponding classical algorithms. It can be considered as a generalization of Grover's algorithm.

Grover's algorithm

Grover's algorithm searches an unstructured database (or an unordered list) with N entries for a marked entry, using only $O(\sqrt{N})$ queries instead of the $O(N)$ queries required classically.[15] Classically, $O(N)$ queries are required even allowing bounded-error probabilistic algorithms.

Theorists have considered a hypothetical generalization of a standard quantum computer that could access the histories of the hidden variables in Bohmian mechanics. (Such a computer is completely hypothetical and would *not* be a standard quantum computer, or even possible under the standard theory of quantum mechanics.) Such a hypothetical computer could implement a search of an N-item database in

at most $O(\sqrt[3]{N})$ steps. This is slightly faster than the $O(\sqrt{N})$ steps taken by Grover's algorithm. However, neither search method would allow either model of quantum computer to solve NP-complete problems in polynomial time.[16]

Quantum counting

Quantum counting solves a generalization of the search problem. It solves the problem of counting the number of marked entries in an unordered list, instead of just detecting whether one exists. Specifically, it counts the number of marked entries in an N-element list with an error of at most ε by making only $\Theta\left(\varepsilon^{-1}\sqrt{N/k}\right)$ queries, where k is the number of marked elements in the list.[17][18] More precisely, the algorithm outputs an estimate k' for k, the number of marked entries, with accuracy $|k-k'| \leq \varepsilon k$.

Algorithms based on quantum walks

A quantum walk is the quantum analogue of a classical random walk. A classical random walk can be described by a probability distribution over some states, while a quantum walk can be described by a quantum superposition over states. Quantum walks are known to give exponential speedups for some black-box problems.[19][20] They also provide polynomial speedups for many problems. A framework for the creation of quantum walk algorithms exists and is a versatile tool.[21]

Boson sampling problem

The Boson Sampling Problem in an experimental configuration assumes[22] an input of bosons (e.g., photons) of moderate number that are randomly scattered into a large number of output modes, constrained by a defined unitarity. When individual photons are used, the problem is isomorphic to a multi-photon quantum walk.[23] The problem is then to produce a fair sample of the probability distribution of the output that depends on the input arrangement of bosons and the unitarity.[24] Solving this problem with a classical computer algorithm requires computing the permanent of the unitary transform matrix, which may take a prohibitively long time or be outright impossible. In 2014, it was proposed[25] that existing technology and standard probabilistic methods of generating single-photon states could be used as an input into a suitable quantum computable linear optical network and that sampling of the output probability distribution would be demonstrably superior using quantum algorithms. In 2015, investigation predicted[26] the sampling problem had similar complexity for inputs other than Fock-state photons and identified a transition in computational complexity from classically simulable to just as hard as the Boson Sampling Problem, depending on the size of coherent amplitude inputs.

Element distinctness problem

The element distinctness problem is the problem of determining whether all the elements of a list are distinct. Classically, $\Omega(N)$ queries are required for a list of size N; however, it can be solved in $\Theta(N^{2/3})$ queries on a quantum computer. The optimal algorithm was put forth by Andris Ambainis,[27]

and Yaoyun Shi first proved a tight lower bound when the size of the range is sufficiently large.[28] Ambainis[29] and Kutin[30] independently (and via different proofs) extended that work to obtain the lower bound for all functions.

Triangle-finding problem

The triangle-finding problem is the problem of determining whether a given graph contains a triangle (a clique of size 3). The best-known lower bound for quantum algorithms is $\Omega(N)$, but the best algorithm known requires O($N^{1.297}$) queries,[31] an improvement over the previous best O($N^{1.3}$) queries.[21][32]

Formula evaluation

A formula is a tree with a gate at each internal node and an input bit at each leaf node. The problem is to evaluate the formula, which is the output of the root node, given oracle access to the input.

A well studied formula is the balanced binary tree with only NAND gates.[33] This type of formula requires $\Theta(N^c)$ queries using randomness,[34] where $c = \log_2(1+\sqrt{33})/4 \approx 0.754$. With a quantum algorithm, however, it can be solved in $\Theta(N^{1/2})$ queries. No better quantum algorithm for this case was known until one was found for the unconventional Hamiltonian oracle model.[7] The same result for the standard setting soon followed.[35]

Fast quantum algorithms for more complicated formulas are also known.[36]

Group commutativity

The problem is to determine if a black-box group, given by *k* generators, is commutative. A black-box group is a group with an oracle function, which must be used to perform the group operations (multiplication, inversion, and comparison with identity). The interest in this context lies in the query complexity, which is the number of oracle calls needed to solve the problem. The deterministic and randomized query complexities are $\Theta(k^2)$ and $\Theta(k)$, respectively.[37] A quantum algorithm requires $\Omega(k^{2/3})$ queries, while the best-known classical algorithm uses $O(k^{2/3}\log k)$ queries.[38]

BQP-complete problems

The complexity class **BQP** (bounded-error quantum polynomial time) is the set of decision problems solvable by a quantum computer in polynomial time with error probability of at most 1/3 for all instances.[39] It is the quantum analogue to the classical complexity class **BPP**.

A problem is **BQP**-complete if it is in **BQP** and any problem in **BQP** can be reduced to it in polynomial time. Informally, the class of **BQP**-complete problems are those that are as hard as the hardest problems in **BQP** and are themselves efficiently solvable by a quantum computer (with bounded error).

Computing knot invariants

Witten had shown that the Chern-Simons topological quantum field theory (TQFT) can be solved in terms of Jones polynomials. A quantum computer can simulate a TQFT, and thereby approximate the Jones polynomial,[40] which as far as we know, is hard to compute classically in the worst-case scenario.

Quantum simulation

The idea that quantum computers might be more powerful than classical computers originated in Richard Feynman's observation that classical computers seem to require exponential time to simulate many-particle quantum systems, yet quantum many-body systems are able to "solve themselves."[41] Since then, the idea that quantum computers can simulate quantum physical processes exponentially faster than classical computers has been greatly fleshed out and elaborated. Efficient (i.e., polynomial-time) quantum algorithms have been developed for simulating both Bosonic and Fermionic systems,[42] as well as the simulation of chemical reactions beyond the capabilities of current classical supercomputers using only a few hundred qubits.[43] Quantum computers can also efficiently simulate topological quantum field theories.[44] In addition to its intrinsic interest, this result has led to efficient quantum algorithms for estimating quantum topological invariants such as Jones[45] and HOMFLY polynomials,[46] and the Turaev-Viro invariant of three-dimensional manifolds.[47]

Solving a linear systems of equations

In 2009, Aram Harrow, Avinatan Hassidim, and Seth Lloyd, formulated a quantum algorithm for solving linear systems. The algorithm estimates the result of a scalar measurement on the solution vector to a given linear system of equations.[48]

Provided that the linear system is sparse and has a low condition number κ, and that the user is interested in the result of a scalar measurement on the solution vector (instead of the values of the solution vector itself), then the algorithm has a runtime of $O(\log(N)\kappa^2)$, where N is the number of variables in the linear system. This offers an exponential speedup over the fastest classical algorithm, which runs in $O(N\kappa)$ (or $O(N\sqrt{\kappa})$ for positive semidefinite matrices).

Hybrid quantum/classical algorithms

Hybrid Quantum/Classical Algorithms combine quantum state preparation and measurement with classical optimization.[49] These algorithms generally aim to determine the ground-state eigenvector and eigenvalue of a Hermitian operator.

QAOA

The quantum approximate optimization algorithm takes inspiration from quantum annealing, performing a discretized approximation of quantum annealing using a quantum circuit. It can be used to solve problems in graph theory.[50] The algorithm makes use of classical optimization of quantum operations to maximize an "objective function."

Variational quantum eigensolver

The variational quantum eigensolver (VQE) algorithm applies classical optimization to minimize the energy expectation value of an ansatz state to find the ground state of a Hermitian operator, such as a molecule's Hamiltonian.[51] It can also be extended to find excited energies of molecular Hamiltonians.[52]

Contracted quantum eigensolver

The contracted quantum eigensolver (CQE) algorithm minimizes the residual of a contraction (or projection) of the Schrödinger equation onto the space of two (or more) electrons to find the ground- or excited-state energy and two-electron reduced density matrix of a molecule.[53] It is based on classical methods for solving energies and two-electron reduced density matrices directly from the anti-Hermitian contracted Schrödinger equation.[54]

See also

- Quantum machine learning
- Quantum optimization algorithms
- Quantum sort
- Primality test

References

1. Nielsen, Michael A.; Chuang, Isaac L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press. ISBN 978-0-521-63503-5.
2. Mosca, M. (2008). "Quantum Algorithms". arXiv:0808.0369 (https://arxiv.org/abs/0808.0369) [quant-ph (https://arxiv.org/archive/quant-ph)].
3. Lanzagorta, Marco; Uhlmann, Jeffrey K. (1 January 2009). *Quantum Computer Science* (https://books.google.com/books?id=-wkJIuw0YRsC&q=quantum%2520computer%2520equivalent%2520classical%2520computer&pg=PA23). Morgan & Claypool Publishers. ISBN 9781598297324.
4. Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information* (https://books.google.com/books?id=-s4DEy7o-a0C) (2nd ed.). Cambridge: Cambridge University Press. ISBN 978-1-107-00217-3.
5. "Shor's algorithm" (https://quantum-computing.ibm.com/docs/iqx/guide/shors-algorithm).
6. "IBM quantum composer user guide: Grover's algorithm" (https://quantum-computing.ibm.com/composer/docs/iqx/guide/grovers-algorithm). *quantum-computing.ibm.com*. Retrieved 7 June 2022.
7. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2008). "A Quantum Algorithm for the Hamiltonian NAND Tree" (https://doi.org/10.4086%2Ftoc.2008.v004a008). *Theory of Computing*. **4**: 169–190. arXiv:quant-ph/0702144 (https://arxiv.org/abs/quant-ph/0702144). doi:10.4086/toc.2008.v004a008 (https://doi.org/10.4086%2Ftoc.2008.v004a008).
8. Childs, Andrew M.; van Dam, W. (2010). "Quantum algorithms for algebraic problems". *Reviews of Modern Physics*. **82** (1): 1–52. arXiv:0812.0380 (https://arxiv.org/abs/0812.0380). Bibcode:2010RvMP...82....1C (https://ui.adsabs.harvard.edu/abs/2010RvMP...82....1C). doi:10.1103/RevModPhys.82.1 (https://doi.org/10.1103%2FRevModPhys.82.1). S2CID 119261679 (https://api.semanticscholar.org/CorpusID:119261679).

9. Shor, P. W. (1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Scientific and Statistical Computing*. **26** (5): 1484–1509. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). Bibcode:1995quant.ph..8027S (https://ui.adsabs.harvard.edu/abs/1995quant.ph..8027S). doi:10.1137/s0097539795293172 (https://doi.org/10.1137%2Fs0097539795293172). S2CID 2337707 (https://api.semanticscholar.org/CorpusID:2337707).
10. Boneh, D.; Lipton, R. J. (1995). "Quantum cryptoanalysis of hidden linear functions". In Coppersmith, D. (ed.). *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*. Springer-Verlag. pp. 424–437. ISBN 3-540-60221-6.
11. Moore, C.; Russell, A.; Schulman, L. J. (2005). "The Symmetric Group Defies Strong Fourier Sampling: Part I". arXiv:quant-ph/0501056 (https://arxiv.org/abs/quant-ph/0501056).
12. Regev, O. (2003). "Quantum Computation and Lattice Problems". arXiv:cs/0304005 (https://arxiv.org/abs/cs/0304005).
13. van Dam, W.; Seroussi, G. (2002). "Efficient Quantum Algorithms for Estimating Gauss Sums". arXiv:quant-ph/0207131 (https://arxiv.org/abs/quant-ph/0207131).
14. Aaronson, S. (2009). "BQP and the Polynomial Hierarchy". arXiv:0910.4698 (https://arxiv.org/abs/0910.4698) [quant-ph (https://arxiv.org/archive/quant-ph)].
15. Grover, Lov K. (1996). "A fast quantum mechanical algorithm for database search". arXiv:quant-ph/9605043 (https://arxiv.org/abs/quant-ph/9605043).
16. Aaronson, Scott. "Quantum Computing and Hidden Variables" (https://www.scottaaronson.com/papers/qchvpra.pdf) (PDF).
17. Brassard, G.; Hoyer, P.; Tapp, A. (1998). "Quantum counting". *Automata, Languages and Programming*. Lecture Notes in Computer Science. Vol. 1443. pp. 820–831. arXiv:quant-ph/9805082 (https://arxiv.org/abs/quant-ph/9805082). doi:10.1007/BFb0055105 (https://doi.org/10.1007%2FBFb0055105). ISBN 978-3-540-64781-2. S2CID 14147978 (https://api.semanticscholar.org/CorpusID:14147978).
18. Brassard, G.; Hoyer, P.; Mosca, M.; Tapp, A. (2002). "Quantum Amplitude Amplification and Estimation". In Samuel J. Lomonaco, Jr. (ed.). *Quantum Computation and Quantum Information*. AMS Contemporary Mathematics. Vol. 305. pp. 53–74. arXiv:quant-ph/0005055 (https://arxiv.org/abs/quant-ph/0005055). Bibcode:2000quant.ph..5055B (https://ui.adsabs.harvard.edu/abs/2000quant.ph..5055B). doi:10.1090/conm/305/05215 (https://doi.org/10.1090%2Fconm%2F305%2F05215). ISBN 9780821821404. S2CID 54753 (https://api.semanticscholar.org/CorpusID:54753).
19. Childs, A. M.; Cleve, R.; Deotto, E.; Farhi, E.; Gutmann, S.; Spielman, D. A. (2003). "Exponential algorithmic speedup by quantum walk". *Proceedings of the 35th Symposium on Theory of Computing*. Association for Computing Machinery. pp. 59–68. arXiv:quant-ph/0209131 (https://arxiv.org/abs/quant-ph/0209131). doi:10.1145/780542.780552 (https://doi.org/10.1145%2F780542.780552). ISBN 1-58113-674-9.
20. Childs, A. M.; Schulman, L. J.; Vazirani, U. V. (2007). "Quantum Algorithms for Hidden Nonlinear Structures". *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*. IEEE. pp. 395–404. arXiv:0705.2784 (https://arxiv.org/abs/0705.2784). doi:10.1109/FOCS.2007.18 (https://doi.org/10.1109%2FFOCS.2007.18). ISBN 978-0-7695-3010-9.
21. Magniez, F.; Nayak, A.; Roland, J.; Santha, M. (2007). "Search via quantum walk". *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*. Association for Computing Machinery. pp. 575–584. arXiv:quant-ph/0608026 (https://arxiv.org/abs/quant-ph/0608026). doi:10.1145/1250790.1250874 (https://doi.org/10.1145%2F1250790.1250874). ISBN 978-1-59593-631-8.

22. Ralph, T.C. (July 2013). "Figure 1: The boson-sampling problem" (http://www.nature.com/nphoton/journal/v7/n7/fig_tab/nphoton.2013.175_F1.html). *Nature Photonics*. **7** (7). Nature: 514–515. doi:10.1038/nphoton.2013.175 (https://doi.org/10.1038%2Fnphoton.2013.175). S2CID 110342419 (https://api.semanticscholar.org/CorpusID:110342419). Retrieved 12 September 2014.
23. Peruzzo, Alberto; Lobino, Mirko; Matthews, Jonathan C. F.; Matsuda, Nobuyuki; Politi, Alberto; Poulios, Konstantinos; Zhou, Xiao-Qi; Lahini, Yoav; Ismail, Nur; Wörhoff, Kerstin; Bromberg, Yaron; Silberberg, Yaron; Thompson, Mark G.; OBrien, Jeremy L. (17 September 2010). "Quantum Walks of Correlated Photons" (https://www.science.org/doi/10.1126/science.1193515). *Science*. **329** (5998): 1500–1503. arXiv:1006.4764 (https://arxiv.org/abs/1006.4764). Bibcode:2010Sci...329.1500P (https://ui.adsabs.harvard.edu/abs/2010Sci...329.1500P). doi:10.1126/science.1193515 (https://doi.org/10.1126%2Fscience.1193515). hdl:10072/53193 (https://hdl.handle.net/10072%2F53193). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 20847264 (https://pubmed.ncbi.nlm.nih.gov/20847264). S2CID 13896075 (https://api.semanticscholar.org/CorpusID:13896075).
24. Lund, A.P.; Laing, A.; Rahimi-Keshari, S.; Rudolph, T.; O'Brien, J.L.; Ralph, T.C. (5 September 2014). "Boson Sampling from Gaussian States". *Phys. Rev. Lett*. **113** (10): 100502. arXiv:1305.4346 (https://arxiv.org/abs/1305.4346). Bibcode:2014PhRvL.113j0502L (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113j0502L). doi:10.1103/PhysRevLett.113.100502 (https://doi.org/10.1103%2FPhysRevLett.113.100502). PMID 25238340 (https://pubmed.ncbi.nlm.nih.gov/25238340). S2CID 27742471 (https://api.semanticscholar.org/CorpusID:27742471).
25. "The quantum revolution is a step closer" (http://phys.org/news/2014-09-quantum-revolution-closer.html). *Phys.org*. Omicron Technology Limited. Retrieved 12 September 2014.
26. Seshadreesan, Kaushik P.; Olson, Jonathan P.; Motes, Keith R.; Rohde, Peter P.; Dowling, Jonathan P. (2015). "Boson sampling with displaced single-photon Fock states versus single-photon-added coherent states: The quantum-classical divide and computational-complexity transitions in linear optics". *Physical Review A*. **91** (2): 022334. arXiv:1402.0531 (https://arxiv.org/abs/1402.0531). Bibcode:2015PhRvA..91b2334S (https://ui.adsabs.harvard.edu/abs/2015PhRvA..91b2334S). doi:10.1103/PhysRevA.91.022334 (https://doi.org/10.1103%2FPhysRevA.91.022334). S2CID 55455992 (https://api.semanticscholar.org/CorpusID:55455992).
27. Ambainis, A. (2007). "Quantum Walk Algorithm for Element Distinctness". *SIAM Journal on Computing*. **37** (1): 210–239. arXiv:quant-ph/0311001 (https://arxiv.org/abs/quant-ph/0311001). doi:10.1137/S0097539705447311 (https://doi.org/10.1137%2FS0097539705447311). S2CID 6581885 (https://api.semanticscholar.org/CorpusID:6581885).
28. Shi, Y. (2002). "Quantum lower bounds for the collision and the element distinctness problems". *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings*. Proceedings of the 43rd Symposium on Foundations of Computer Science. pp. 513–519. arXiv:quant-ph/0112086 (https://arxiv.org/abs/quant-ph/0112086). doi:10.1109/SFCS.2002.1181975 (https://doi.org/10.1109%2FSFCS.2002.1181975). ISBN 0-7695-1822-2.
29. Ambainis, A. (2005). "Polynomial Degree and Lower Bounds in Quantum Complexity: Collision and Element Distinctness with Small Range" (https://doi.org/10.4086%2Ftoc.2005.v001a003). *Theory of Computing*. **1** (1): 37–46. doi:10.4086/toc.2005.v001a003 (https://doi.org/10.4086%2Ftoc.2005.v001a003).
30. Kutin, S. (2005). "Quantum Lower Bound for the Collision Problem with Small Range" (https://doi.org/10.4086%2Ftoc.2005.v001a002). *Theory of Computing*. **1** (1): 29–36. doi:10.4086/toc.2005.v001a002 (https://doi.org/10.4086%2Ftoc.2005.v001a002).
31. Aleksandrs Belovs (2011). "Span Programs for Functions with Constant-Sized 1-certificates". arXiv:1105.4024 (https://arxiv.org/abs/1105.4024) [quant-ph (https://arxiv.org/archive/quant-ph)].

32. Magniez, F.; Santha, M.; Szegedy, M. (2007). "Quantum Algorithms for the Triangle Problem". *SIAM Journal on Computing*. **37** (2): 413–424. arXiv:quant-ph/0310134 (https://arxiv.org/abs/quant-ph/0310134). doi:10.1137/050643684 (https://doi.org/10.1137%2F050643684). S2CID 594494 (https://api.semanticscholar.org/CorpusID:594494).
33. Aaronson, S. (3 February 2007). "NAND now for something completely different" (http://scottaaronson.com/blog/?p=207). *Shtetl-Optimized*. Retrieved 17 December 2009.
34. Saks, M.E.; Wigderson, A. (1986). "Probabilistic Boolean Decision Trees and the Complexity of Evaluating Game Trees" (http://www.math.ias.edu/~avi/PUBLICATIONS/MYPAPERS/SW86/SW86.pdf) (PDF). *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*. IEEE. pp. 29–38. doi:10.1109/SFCS.1986.44 (https://doi.org/10.1109%2FSFCS.1986.44). ISBN 0-8186-0740-8.
35. Ambainis, A. (2007). "A nearly optimal discrete query quantum algorithm for evaluating NAND formulas". arXiv:0704.3628 (https://arxiv.org/abs/0704.3628) [quant-ph (https://arxiv.org/archive/quant-ph)].
36. Reichardt, B. W.; Spalek, R. (2008). "Span-program-based quantum algorithm for evaluating formulas". *Proceedings of the 40th Annual ACM symposium on Theory of Computing*. Association for Computing Machinery. pp. 103–112. arXiv:0710.2630 (https://arxiv.org/abs/0710.2630). doi:10.1145/1374376.1374394 (https://doi.org/10.1145%2F1374376.1374394). ISBN 978-1-60558-047-0.
37. Pak, Igor (2012). "Testing commutativity of a group and the power of randomization" (https://doi.org/10.1112%2FS1461157012000046). *LMS Journal of Computation and Mathematics*. **15**: 38–43. doi:10.1112/S1461157012000046 (https://doi.org/10.1112%2FS1461157012000046).
38. Magniez, F.; Nayak, A. (2007). "Quantum Complexity of Testing Group Commutativity". *Algorithmica*. **48** (3): 221–232. arXiv:quant-ph/0506265 (https://arxiv.org/abs/quant-ph/0506265). doi:10.1007/s00453-007-0057-8 (https://doi.org/10.1007%2Fs00453-007-0057-8). S2CID 3163328 (https://api.semanticscholar.org/CorpusID:3163328).
39. Michael Nielsen and Isaac Chuang (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. ISBN 0-521-63503-9.
40. Aharonov, D.; Jones, V.; Landau, Z. (2006). "A polynomial quantum algorithm for approximating the Jones polynomial". *Proceedings of the 38th Annual ACM symposium on Theory of Computing*. Association for Computing Machinery. pp. 427–436. arXiv:quant-ph/0511096 (https://arxiv.org/abs/quant-ph/0511096). doi:10.1145/1132516.1132579 (https://doi.org/10.1145%2F1132516.1132579). ISBN 1595931341.
41. Feynman, R. P. (1982). "Simulating physics with computers". *International Journal of Theoretical Physics*. **21** (6–7): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). CiteSeerX 10.1.1.45.9310 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9310). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445).
42. Abrams, D. S.; Lloyd, S. (1997). "Simulation of many-body Fermi systems on a universal quantum computer". *Physical Review Letters*. **79** (13): 2586–2589. arXiv:quant-ph/9703054 (https://arxiv.org/abs/quant-ph/9703054). Bibcode:1997PhRvL..79.2586A (https://ui.adsabs.harvard.edu/abs/1997PhRvL..79.2586A). doi:10.1103/PhysRevLett.79.2586 (https://doi.org/10.1103%2FPhysRevLett.79.2586). S2CID 18231521 (https://api.semanticscholar.org/CorpusID:18231521).
43. Kassal, I.; Jordan, S. P.; Love, P. J.; Mohseni, M.; Aspuru-Guzik, A. (2008). "Polynomial-time quantum algorithm for the simulation of chemical dynamics" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2596249). *Proceedings of the National Academy of Sciences of the United States of America*. **105** (48): 18681–86. arXiv:0801.2986 (https://arxiv.org/abs/0801.2986). Bibcode:2008PNAS..10518681K (https://ui.adsabs.harvard.edu/abs/2008PNAS..10518681K). doi:10.1073/pnas.0808245105 (https://doi.org/10.1073%2Fpnas.0808245105). PMC 2596249 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2596249). PMID 19033207 (https://pubmed.ncbi.nlm.nih.gov/19033207).

44. Freedman, M.; Kitaev, A.; Wang, Z. (2002). "Simulation of Topological Field Theories by Quantum Computers". *Communications in Mathematical Physics*. **227** (3): 587–603. arXiv:quant-ph/0001071 (https://arxiv.org/abs/quant-ph/0001071). Bibcode:2002CMaPh.227..587F (https://ui.adsabs.harvard.edu/abs/2002CMaPh.227..587F). doi:10.1007/s002200200635 (https://doi.org/10.1007%2Fs002200200635). S2CID 449219 (https://api.semanticscholar.org/CorpusID:449219).
45. Aharonov, D.; Jones, V.; Landau, Z. (2009). "A polynomial quantum algorithm for approximating the Jones polynomial". *Algorithmica*. **55** (3): 395–421. arXiv:quant-ph/0511096 (https://arxiv.org/abs/quant-ph/0511096). doi:10.1007/s00453-008-9168-0 (https://doi.org/10.1007%2Fs00453-008-9168-0). S2CID 7058660 (https://api.semanticscholar.org/CorpusID:7058660).
46. Wocjan, P.; Yard, J. (2008). "The Jones polynomial: quantum algorithms and applications in quantum complexity theory". *Quantum Information and Computation*. **8** (1): 147–180. arXiv:quant-ph/0603069 (https://arxiv.org/abs/quant-ph/0603069). Bibcode:2006quant.ph..3069W (https://ui.adsabs.harvard.edu/abs/2006quant.ph..3069W). doi:10.26421/QIC8.1-2-10 (https://doi.org/10.26421%2FQIC8.1-2-10). S2CID 14494227 (https://api.semanticscholar.org/CorpusID:14494227).
47. Alagic, G.; Jordan, S.P.; König, R.; Reichardt, B. W. (2010). "Approximating Turaev-Viro 3-manifold invariants is universal for quantum computation". *Physical Review A*. **82** (4): 040302. arXiv:1003.0923 (https://arxiv.org/abs/1003.0923). Bibcode:2010PhRvA..82d0302A (https://ui.adsabs.harvard.edu/abs/2010PhRvA..82d0302A). doi:10.1103/PhysRevA.82.040302 (https://doi.org/10.1103%2FPhysRevA.82.040302). S2CID 28281402 (https://api.semanticscholar.org/CorpusID:28281402).
48. Harrow, Aram W; Hassidim, Avinatan; Lloyd, Seth (2008). "Quantum algorithm for solving linear systems of equations". *Physical Review Letters*. **103** (15): 150502. arXiv:0811.3171 (https://arxiv.org/abs/0811.3171). Bibcode:2009PhRvL.103o0502H (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103o0502H). doi:10.1103/PhysRevLett.103.150502 (https://doi.org/10.1103%2FPhysRevLett.103.150502). PMID 19905613 (https://pubmed.ncbi.nlm.nih.gov/19905613). S2CID 5187993 (https://api.semanticscholar.org/CorpusID:5187993).
49. Moll, Nikolaj; Barkoutsos, Panagiotis; Bishop, Lev S.; Chow, Jerry M.; Cross, Andrew; Egger, Daniel J.; Filipp, Stefan; Fuhrer, Andreas; Gambetta, Jay M.; Ganzhorn, Marc; Kandala, Abhinav; Mezzacapo, Antonio; Müller, Peter; Riess, Walter; Salis, Gian; Smolin, John; Tavernelli, Ivano; Temme, Kristan (2018). "Quantum optimization using variational algorithms on near-term quantum devices". *Quantum Science and Technology*. **3** (3): 030503. arXiv:1710.01022 (https://arxiv.org/abs/1710.01022). Bibcode:2018QS&T....3c0503M (https://ui.adsabs.harvard.edu/abs/2018QS&T....3c0503M). doi:10.1088/2058-9565/aab822 (https://doi.org/10.1088%2F2058-9565%2Faab822). S2CID 56376912 (https://api.semanticscholar.org/CorpusID:56376912).
50. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (14 November 2014). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
51. Peruzzo, Alberto; McClean, Jarrod; Shadbolt, Peter; Yung, Man-Hong; Zhou, Xiao-Qi; Love, Peter J.; Aspuru-Guzik, Alán; O'Brien, Jeremy L. (23 July 2014). "A variational eigenvalue solver on a photonic quantum processor" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4124861). *Nature Communications*. **5** (1): 4213. arXiv:1304.3061 (https://arxiv.org/abs/1304.3061). Bibcode:2014NatCo...5.4213P (https://ui.adsabs.harvard.edu/abs/2014NatCo...5.4213P). doi:10.1038/ncomms5213 (https://doi.org/10.1038%2Fncomms5213). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 4124861 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4124861). PMID 25055053 (https://pubmed.ncbi.nlm.nih.gov/25055053).

52. Higgott, Oscar; Wang, Daochen; Brierley, Stephen (2019). "Variational Quantum Computation of Excited States". *Quantum*. **3**: 156. arXiv:1805.08138 (https://arxiv.org/abs/1805.08138). Bibcode:2019Quant...3..156H (https://ui.adsabs.harvard.edu/abs/2019Quant...3..156H). doi:10.22331/q-2019-07-01-156 (https://doi.org/10.22331%2Fq-2019-07-01-156). S2CID 119185497 (https://api.semanticscholar.org/CorpusID:119185497).
53. Smart, Scott; Mazziotti, David (18 February 2021). "Quantum Solver of Contracted Eigenvalue Equations for Scalable Molecular Simulations on Quantum Computing Devices". *Phys. Rev. Lett*. **125** (7): 070504. arXiv:2004.11416 (https://arxiv.org/abs/2004.11416). Bibcode:2021PhRvL.126g0504S (https://ui.adsabs.harvard.edu/abs/2021PhRvL.126g0504S). doi:10.1103/PhysRevLett.126.070504 (https://doi.org/10.1103%2FPhysRevLett.126.070504). PMID 33666467 (https://pubmed.ncbi.nlm.nih.gov/33666467). S2CID 216144443 (https://api.semanticscholar.org/CorpusID:216144443).
54. Mazziotti, David (6 October 2006). "Anti-Hermitian Contracted Schrödinger Equation: Direct Determination of the Two-Electron Reduced Density Matrices of Many-Electron Molecules". *Phys. Rev. Lett*. **97** (14): 143002. Bibcode:2006PhRvL..97n3002M (https://ui.adsabs.harvard.edu/abs/2006PhRvL..97n3002M). doi:10.1103/PhysRevLett.97.143002 (https://doi.org/10.1103%2FPhysRevLett.97.143002). PMID 17155245 (https://pubmed.ncbi.nlm.nih.gov/17155245).

External links

- The Quantum Algorithm Zoo (https://quantumalgorithmzoo.org): A comprehensive list of quantum algorithms that provide a speedup over the fastest known classical algorithms.
- Andrew Childs' lecture notes on quantum algorithms (https://www.cs.umd.edu/~amchilds/qa/)
- The Quantum search algorithm - brute force (https://bastion.center/the-quantum-search-algorithm/) Archived (https://web.archive.org/web/20180901034619/https://bastion.center/the-quantum-search-algorithm/) 1 September 2018 at the Wayback Machine.

Surveys

- Dalzell, Alexander M.; et al. (2023). "Quantum algorithms: A survey of applications and end-to-end complexities". arXiv:2310.03011 (https://arxiv.org/abs/2310.03011) [quant-ph (https://arxiv.org/archive/quant-ph)].
- Smith, J.; Mosca, M. (2012). "Algorithms for Quantum Computers". *Handbook of Natural Computing*. pp. 1451–1492. arXiv:1001.0767 (https://arxiv.org/abs/1001.0767). doi:10.1007/978-3-540-92910-9_43 (https://doi.org/10.1007%2F978-3-540-92910-9_43). ISBN 978-3-540-92909-3. S2CID 16565723 (https://api.semanticscholar.org/CorpusID:16565723).
- Childs, A. M.; Van Dam, W. (2010). "Quantum algorithms for algebraic problems". *Reviews of Modern Physics*. **82** (1): 1–52. arXiv:0812.0380 (https://arxiv.org/abs/0812.0380). Bibcode:2010RvMP...82....1C (https://ui.adsabs.harvard.edu/abs/2010RvMP...82....1C). doi:10.1103/RevModPhys.82.1 (https://doi.org/10.1103%2FRevModPhys.82.1). S2CID 119261679 (https://api.semanticscholar.org/CorpusID:119261679).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_algorithm&oldid=1221761276"

WIKIPEDIA
The Free Encyclopedia

Amplitude amplification

Amplitude amplification is a technique in quantum computing which generalizes the idea behind Grover's search algorithm, and gives rise to a family of quantum algorithms. It was discovered by Gilles Brassard and Peter Høyer in 1997,[1] and independently rediscovered by Lov Grover in 1998.[2]

In a quantum computer, amplitude amplification can be used to obtain a quadratic speedup over several classical algorithms.

Algorithm

The derivation presented here roughly follows the one given by Brassard et al. in 2000.[3] Assume we have an N-dimensional Hilbert space $\mathcal{H}$ representing the state space of a quantum system, spanned by the orthonormal computational basis states $B := \{|k\rangle\}_{k=0}^{N-1}$. Furthermore assume we have a Hermitian projection operator $P: \mathcal{H} \to \mathcal{H}$. Alternatively, P may be given in terms of a Boolean oracle function $\chi: \mathbb{Z} \to \{0, 1\}$ and an orthonormal operational basis $B_{\text{op}} := \{|\omega_k\rangle\}_{k=0}^{N-1}$, in which case

$$P := \sum_{\chi(k)=1} |\omega_k\rangle\langle\omega_k|.$$

P can be used to partition $\mathcal{H}$ into a direct sum of two mutually orthogonal subspaces, the *good* subspace $\mathcal{H}_1$ and the *bad* subspace $\mathcal{H}_0$:

$$\begin{aligned}\mathcal{H}_1 &:= \operatorname{Image} P &&= \operatorname{span}\{|\omega_k\rangle \in B_{\text{op}} \mid \chi(k) = 1\},\\ \mathcal{H}_0 &:= \operatorname{Ker} P &&= \operatorname{span}\{|\omega_k\rangle \in B_{\text{op}} \mid \chi(k) = 0\}.\end{aligned}$$

In other words, we are defining a "*good subspace*" $\mathcal{H}_1$ via the projector P. The goal of the algorithm is then to evolve some initial state $|\psi\rangle \in \mathcal{H}$ into a state belonging to $\mathcal{H}_1$.

Given a normalized state vector $|\psi\rangle \in \mathcal{H}$ with nonzero overlap with both subspaces, we can uniquely decompose it as

$$|\psi\rangle = \sin(\theta)|\psi_1\rangle + \cos(\theta)|\psi_0\rangle,$$

where $\theta = \arcsin(|P|\psi\rangle|) \in [0, \pi/2]$, and $|\psi_1\rangle$ and $|\psi_0\rangle$ are the normalized projections of $|\psi\rangle$ into the subspaces $\mathcal{H}_1$ and $\mathcal{H}_0$, respectively. This decomposition defines a two-dimensional subspace $\mathcal{H}_\psi$, spanned by the vectors $|\psi_0\rangle$ and $|\psi_1\rangle$. The probability of finding the system in a *good* state when measured is $\sin^2(\theta)$.

Define a unitary operator $Q(\psi, P) := -S_\psi S_P$, where

$$\begin{aligned}S_\psi &= I - 2|\psi\rangle\langle\psi| \quad \text{and}\\ S_P &= I - 2P.\end{aligned}$$

S_P flips the phase of the states in the *good* subspace, whereas S_ψ flips the phase of the initial state $|\psi\rangle$.

The action of this operator on $\mathcal{H}_\psi$ is given by

$$Q|\psi_0\rangle = -S_\psi|\psi_0\rangle = (2\cos^2(\theta) - 1)|\psi_0\rangle + 2\sin(\theta)\cos(\theta)|\psi_1\rangle \text{ and}$$
$$Q|\psi_1\rangle = S_\psi|\psi_1\rangle = -2\sin(\theta)\cos(\theta)|\psi_0\rangle + (1 - 2\sin^2(\theta))|\psi_1\rangle.$$

Thus in the $\mathcal{H}_\psi$ subspace Q corresponds to a rotation by the angle 2θ:

$$Q = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}.$$

Applying Q n times on the state $|\psi\rangle$ gives

$$Q^n|\psi\rangle = \cos((2n+1)\theta)|\psi_0\rangle + \sin((2n+1)\theta)|\psi_1\rangle,$$

rotating the state between the *good* and *bad* subspaces. After n iterations the probability of finding the system in a *good* state is $\sin^2((2n+1)\theta)$.
The probability is maximized if we choose

$$n = \left\lfloor \frac{\pi}{4\theta} \right\rfloor.$$

Up until this point each iteration increases the amplitude of the *good* states, hence the name of the technique.

Applications

Assume we have an unsorted database with N elements, and an oracle function χ which can recognize the *good* entries we are searching for, and $B_{\text{op}} = B$ for simplicity.

If there are G *good* entries in the database in total, then we can find them by initializing a quantum register $|\psi\rangle$ with n qubits where $2^n = N$ into a uniform superposition of all the database elements N such that

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle$$

and running the above algorithm. In this case the overlap of the initial state with the *good* subspace is equal to the square root of the frequency of the *good* entries in the database, $\sin(\theta) = |P|\psi\rangle| = \sqrt{G/N}$. If $\sin(\theta) \ll 1$, we can approximate the number of required iterations as

$$n = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \approx \left\lfloor \frac{\pi}{4\sin(\theta)} \right\rfloor = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{G}} \right\rfloor = O(\sqrt{N}).$$

Measuring the state will now give one of the *good* entries with high probability. Since each application of S_P requires a single oracle query (assuming that the oracle is implemented as a quantum gate), we can find a *good* entry with just $O(\sqrt{N})$ oracle queries, thus obtaining a quadratic speedup over the best

possible classical algorithm. (The classical method for searching the database would be to perform the query for every $e \in \{0, 1, \ldots, N-1\}$ until a solution is found, thus costing $O(N)$ queries.) Moreover, we can find all G solutions using $O(\sqrt{GN})$ queries.

If we set the size of the set G to one, the above scenario essentially reduces to the original Grover search.

Quantum counting

Suppose that the number of *good* entries is unknown. We aim to estimate $\tilde{G}$ such that $(1-\delta)G \leq \tilde{G} \leq (1+\delta)G$ for small $\delta > 0$. We can solve for $\tilde{G}$ by applying the quantum phase estimation algorithm on unitary operator Q.

Since $e^{2i\theta}$ and $e^{-2i\theta}$ are the only two eigenvalues of Q, we can let their corresponding eigenvectors be $|\psi_1\rangle$ and $|\psi_2\rangle$. We can find the eigenvalue $e^{2i\theta}$ of $|\psi\rangle$, which in this case is equivalent to estimating the phase θ. This can be done by applying Fourier transforms and controlled unitary operations, as described in the quantum phase estimation algorithm. With the estimate $\tilde{\theta}$, we can estimate $\sin\theta$, which in turn estimates G.

Suppose we want to estimate θ with arbitrary starting state $|s\rangle$, instead of the eigenvectors $|\psi_1\rangle$ and $|\psi_2\rangle$. We can do this by decomposing $|s\rangle$ into a linear combination of $|\psi_1\rangle$ and $|\psi_2\rangle$, and then applying the phase estimation algorithm.

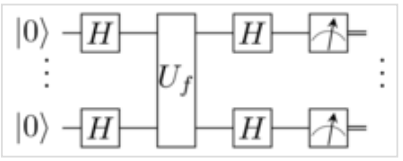
References

1. Gilles Brassard; Peter Høyer (June 1997). "An exact quantum polynomial-time algorithm for Simon's problem". *Proceedings of the Fifth Israeli Symposium on Theory of Computing and Systems*. IEEE Computer Society Press. pp. 12–23. arXiv:quant-ph/9704027 (https://arxiv.org/abs/quant-ph/9704027). Bibcode:1997quant.ph..4027B (https://ui.adsabs.harvard.edu/abs/1997quant.ph..4027B). doi:10.1109/ISTCS.1997.595153 (https://doi.org/10.1109%2FISTCS.1997.595153). ISBN 0-8186-8037-7. S2CID 5177739 (https://api.semanticscholar.org/CorpusID:5177739).
2. Grover, Lov K. (May 1998). "Quantum Computers Can Search Rapidly by Using Almost Any Transformation". *Phys. Rev. Lett*. **80** (19): 4329–4332. arXiv:quant-ph/9712011 (https://arxiv.org/abs/quant-ph/9712011). Bibcode:1998PhRvL..80.4329G (https://ui.adsabs.harvard.edu/abs/1998PhRvL..80.4329G). doi:10.1103/PhysRevLett.80.4329 (https://doi.org/10.1103%2FPhysRevLett.80.4329). S2CID 17879840 (https://api.semanticscholar.org/CorpusID:17879840).
3. Gilles Brassard; Peter Høyer; Michele Mosca; Alain Tapp (2000-05-15). "Quantum amplitude amplification and estimation". *Quantum Computation and Information*. Contemporary Mathematics. Vol. 305. pp. 53–74. arXiv:quant-ph/0005055 (https://arxiv.org/abs/quant-ph/0005055). doi:10.1090/conm/305/05215 (https://doi.org/10.1090%2Fconm%2F305%2F05215). ISBN 9780821821404. S2CID 54753 (https://api.semanticscholar.org/CorpusID:54753).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Amplitude_amplification&oldid=1186099759"

WIKIPEDIA
The Free Encyclopedia

Bernstein–Vazirani algorithm



The **Bernstein–Vazirani algorithm**, which solves the **Bernstein–Vazirani problem**, is a quantum algorithm invented by Ethan Bernstein and Umesh Vazirani in 1997.[1] It is a restricted version of the Deutsch–Jozsa algorithm where instead of distinguishing between two different classes of functions, it tries to learn a string encoded in a function.[2] The Bernstein–Vazirani algorithm was designed to prove an oracle separation between complexity classes BQP and BPP.[1]

Problem statement

Given an oracle that implements a function $f\colon \{0,1\}^n \to \{0,1\}$ in which $f(x)$ is promised to be the dot product between x and a secret string $s \in \{0,1\}^n$ modulo 2, $f(x) = x \cdot s = x_1 s_1 \oplus x_2 s_2 \oplus \cdots \oplus x_n s_n$, find s.

Algorithm

Classically, the most efficient method to find the secret string is by evaluating the function n times with the input values $x = 2^i$ for all $i \in \{0, 1, \ldots, n-1\}$:[2]

$$\begin{aligned} f(1000\cdots 0_n) &= s_1 \\ f(0100\cdots 0_n) &= s_2 \\ f(0010\cdots 0_n) &= s_3 \\ &\vdots \\ f(0000\cdots 1_n) &= s_n \end{aligned}$$

In contrast to the classical solution which needs at least n queries of the function to find s, only one query is needed using quantum computing. The quantum algorithm is as follows: [2]

Apply a Hadamard transform to the n qubit state $|0\rangle^{\otimes n}$ to get

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

Next, apply the oracle U_f which transforms $|x\rangle \to (-1)^{f(x)}|x\rangle$. This can be simulated through the standard oracle that transforms $|b\rangle|x\rangle \to |b \oplus f(x)\rangle|x\rangle$ by applying this oracle to $\frac{|0\rangle - |1\rangle}{\sqrt{2}}|x\rangle$. ($\oplus$ denotes addition mod two.) This transforms the superposition into

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle.$$

Another Hadamard transform is applied to each qubit which makes it so that for qubits where $s_i = 1$, its state is converted from $|-\rangle$ to $|1\rangle$ and for qubits where $s_i = 0$, its state is converted from $|+\rangle$ to $|0\rangle$. To obtain s, a measurement in the standard basis ($\{|0\rangle, |1\rangle\}$) is performed on the qubits.

Graphically, the algorithm may be represented by the following diagram, where $H^{\otimes n}$ denotes the Hadamard transform on n qubits:

$$|0\rangle^n \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} |y\rangle = |s\rangle$$

The reason that the last state is $|s\rangle$ is because, for a particular y,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot s + x \cdot y} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot (s \oplus y)} = 1 \text{ if } s \oplus y = \vec{0}, \text{ 0 otherwise.}$$

Since $s \oplus y = \vec{0}$ is only true when $s = y$, this means that the only non-zero amplitude is on $|s\rangle$. So, measuring the output of the circuit in the computational basis yields the secret string s.

A generalization of Bernstein–Vazirani problem has been proposed that involves finding one or more secret keys using a probabilistic oracle. [3] This is an interesting problem for which a quantum algorithm can provide efficient solutions with certainty or with a high degree of confidence, while classical algorithms completely fail to solve the problem in the general case.

See also

- Hidden Linear Function problem

References

1. Ethan Bernstein and Umesh Vazirani (1997). "Quantum Complexity Theory". *SIAM Journal on Computing*. **26** (5): 1411–1473. doi:10.1137/S0097539796300921 (https://doi.org/10.1137%2FS0097539796300921).
2. S D Fallek, C D Herold, B J McMahon, K M Maller, K R Brown, and J M Amini (2016). "Transport implementation of the Bernstein–Vazirani algorithm with ion qubits" (https://doi.org/10.1088%2F1367-2630%2Faab341). *New Journal of Physics*. **18**. arXiv:1710.01378 (https://arxiv.org/abs/1710.01378). doi:10.1088/1367-2630/aab341 (https://doi.org/10.1088%2F1367-2630%2Faab341).
3. Alok Shukla and Prakash Vedula (2023). "A generalization of Bernstein--Vazirani algorithm with multiple secret keys and a probabilistic oracle". *Quantum Information Processing*. 22:244 (6): 1–18. arXiv:2301.10014 (https://arxiv.org/abs/2301.10014). doi:10.1007/s11128-023-03978-3 (https://doi.org/10.1007%2Fs11128-023-03978-3).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Bernstein–Vazirani_algorithm&oldid=1229696780"

WIKIPEDIA
The Free Encyclopedia

Boson sampling

Boson sampling is a restricted model of non-universal quantum computation introduced by Scott Aaronson and Alex Arkhipov[1] after the original work of Lidror Troyansky and Naftali Tishby, that explored possible usage of boson scattering to evaluate expectation values of permanents of matrices.[2] The model consists of sampling from the probability distribution of identical bosons scattered by a linear interferometer. Although the problem is well defined for any bosonic particles, its photonic version is currently considered as the most promising platform for a scalable implementation of a boson sampling device, which makes it a non-universal approach to linear optical quantum computing. Moreover, while not universal, the boson sampling scheme is strongly believed to implement computing tasks which are hard to implement with classical computers by using far fewer physical resources than a full linear-optical quantum computing setup. This advantage makes it an ideal candidate for demonstrating the power of quantum computation in the near term.

Description

Consider a multimode linear-optical circuit of N modes that is injected with M indistinguishable single photons ($N>M$). Then, the photonic implementation of the boson sampling task consists of generating a sample from the probability distribution of single-photon measurements at the output of the circuit. Specifically, this requires reliable sources of single photons (currently the most widely used ones are parametric down-conversion crystals), as well as a linear interferometer. The latter can be fabricated, e.g., with fused-fiber beam splitters,[3] through silica-on-silicon[4] or laser-written[5][6][7] integrated interferometers, or electrically and optically interfaced optical chips.[8] Finally, the scheme also necessitates high efficiency single photon-counting detectors, such as those based on current-biased superconducting nanowires, which perform the measurements at the output of the circuit. Therefore, based on these three ingredients, the boson sampling setup does not require any ancillas, adaptive measurements or entangling operations, as does e.g. the universal optical scheme by Knill, Laflamme and Milburn (the **KLM** scheme). This makes it a non-universal model of quantum computation, and reduces the amount of physical resources needed for its practical realization.

Specifically, suppose the linear interferometer is described by an $N\times N$ unitary matrix U, which performs a linear transformation of the creation (annihilation) operators $a_i^\dagger$ (a_i) of the circuit's input modes:

$$b_j^\dagger = \sum_{i=1}^{N} U_{ji} a_i^\dagger \quad (b_j = \sum_{i=1}^{N} U_{ji}^* a_i).$$

Here i (j) labels the input (output) modes, and $b_j^\dagger$ (b_j) denotes the creation (annihilation) operators of the output modes ($i,j=1,\ldots, N$). An interferometer characterized by some unitary U naturally induces a unitary evolution $\varphi_M(U)$ on M-photon states. Moreover, the map φ_M is a homomorphism between N-dimensional unitary matrices, and unitaries acting on the exponentially large Hilbert space of the system:

simple counting arguments show that the size of the Hilbert space corresponding to a system of M indistinguishable photons distributed among N modes is given by the binomial coefficient $\binom{M+N-1}{M}$ (notice that since this homomorphism exists, not all values of W are possible).

Suppose the interferometer is injected with an input state of single photons $|\psi_{\text{in}}\rangle = |s_1, s_2, \ldots, s_N\rangle$ with $\sum_{k=1}^{N} s_k = M$ (s_k is the number of photons injected into the kth mode). Then, the state $|\psi_{\text{out}}\rangle$ at

the output of the circuit can be written down as $|\psi_{\text{out}}\rangle = \varphi_M(U)|s_1, s_2, \ldots, s_N\rangle$. A simple way to understand the homomorphism between U and $\varphi_M(U)$ is the following :

We define the isomorphism for the basis states: $P_{|s_1,s_2,\ldots,s_N\rangle}(\mathbf{x}) \equiv x_1^{s_1} \cdot x_2^{s_2} \cdots x_N^{s_N}$, and get the following result : $P_{\varphi(U)|s_1,s_2,\ldots,s_N\rangle}(\mathbf{x}) = P_{|s_1,s_2,\ldots,s_N\rangle}(U\mathbf{x})$

Consequently, the probability $p(t_1, t_2, \ldots, t_N)$ of detecting t_k photons at the kth output mode is given as[9]

$$p(t_1, t_2, \ldots, t_N) = |\langle t_1, t_2, \ldots, t_N|\psi_{\text{out}}\rangle|^2 = \frac{|\operatorname{Perm} U_{S,T}|^2}{t_1! \cdots t_N! s_1! \cdots s_N!}.$$

In the above expression $\operatorname{Perm} U_{S,T}$ stands for the permanent of the matrix $U_{S,T}$, which is obtained from the unitary U by repeating s_i times its ith column and t_j times its jth row. Usually, in the context of the boson sampling problem the input state is taken of a standard form, denoted as $|1_M\rangle$, for which each of the first M modes of the interferometer is injected with a single photon. In this case the above expression reads:

$$p(t_1, t_2, \ldots, t_N) = |\langle t_1, t_2, \ldots, t_N|\varphi_M(U)|1_M\rangle|^2 = \frac{|\operatorname{Perm} U_T|^2}{t_1! \cdots t_N!},$$

where the matrix U_T is obtained from U by keeping its first M columns and repeating t_j times its jth row. Subsequently, the task of boson sampling is to sample either exactly or approximately from the above output distribution, given the unitary U describing the linear-optical circuit as input. As detailed below, the appearance of the permanent in the corresponding statistics of single-photon measurements contributes to the hardness of the boson sampling problem.

Complexity of the problem

The main reason of the growing interest towards the model of boson sampling is that despite being non-universal it is strongly believed to perform a computational task that is intractable for a classical computer. One of the main reasons behind this is that the probability distribution, which the boson sampling device has to sample from, is related to the permanent of complex matrices. The computation of the permanent is in the general case an extremely hard task: it falls in the #P-hard complexity class. Moreover, its approximation to within multiplicative error is a #P-hard problem as well.

All current proofs of the hardness of simulating boson sampling on a classical computer rely on the strong computational consequences that its efficient simulation by a classical algorithm would have. Namely, these proofs show that an efficient classical simulation would imply the collapse of the polynomial hierarchy to its third level, a possibility that is considered very unlikely by the computer science community, due to its strong computational implications (in line with the strong implications of P=NP problem).

Exact sampling

The hardness proof of the exact boson sampling problem can be achieved following two distinct paths. Specifically, the first one uses the tools of the computational complexity theory and combines the following two facts:

1. Approximating the probability $p(t_1, t_2, \ldots, t_N)$ of a specific measurement outcome at the output of a linear interferometer to within a multiplicative constant is a #P-hard problem (due to the complexity of the permanent)
2. If a polynomial-time classical algorithm for exact boson sampling existed, then the above probability $p(t_1, t_2, \ldots, t_N)$ could have been approximated to within a multiplicative constant in the $\mathrm{BPP}^{\mathrm{NP}}$complexity class,[10] i.e. within the third level of the polynomial hierarchy

When combined these two facts along with Toda's theorem result in the collapse of the polynomial hierarchy, which as mentioned above is highly unlikely to occur. This leads to the conclusion that there is no classical polynomial-time algorithm for the exact boson sampling problem.

On the other hand, the alternative proof is inspired by a similar result for another restricted model of quantum computation – the model of instantaneous quantum computing.[11] Namely, the proof uses the KLM scheme, which says that linear optics with adaptive measurements is universal for the class BQP. It also relies on the following facts:

1. Linear optics with postselected measurements is universal for PostBQP, i.e. quantum polynomial-time class with postselection (a straightforward corollary of the KLM construction)
2. The class PostBQP is equivalent to PP (i.e. the probabilistic polynomial-time class): PostBQP = PP[12]
3. The existence of a classical boson sampling algorithm implies the simulability of postselected linear optics in the PostBPP class (that is, classical polynomial-time with postselection, known also as the class $\mathrm{BPP}_{\mathrm{path}}$)

Again, the combination of these three results, as in the previous case, results in the collapse of the polynomial hierarchy. This makes the existence of a classical polynomial-time algorithm for the exact boson sampling problem highly unlikely.

The best proposed classical algorithm for exact boson sampling runs in time $O(n2^n + mn^2)$ for a system with *n* photons and *m* output modes.[13] This algorithm leads to an estimate of 50 photons required to demonstrate quantum supremacy with boson sampling. There is also an open-source implementation (https://CRAN.R-project.org/package=BosonSampling) in R.

Approximate sampling

The above hardness proofs are not applicable to the realistic implementation of a boson sampling device, due to the imperfection of any experimental setup (including the presence of noise, decoherence, photon losses, etc.). Therefore, for practical needs one necessitates the hardness proof for the corresponding approximate task. The latter consists of sampling from a probability distribution that is ε close to the one given by $p(t_1, t_2, \ldots, t_N)$, in terms of the total variation distance. The understanding of the complexity of this problem relies then on several additional assumptions, as well as on two yet unproven conjectures.

Specifically, the proofs of the exact boson sampling problem cannot be directly applied here, since they are based on the #P-hardness of estimating the exponentially-small probability $p(t_1, t_2, \ldots, t_N)$ of a specific measurement outcome. Thus, if a sampler "*knew*" which $p(t_1, t_2, \ldots, t_N)$ we wanted to estimate, then it could adversarially choose to corrupt it (as long as the task is approximate). That is why, the idea is to "*hide*" the above probability $p(t_1, t_2, \ldots, t_N)$ into an $N \times N$ random unitary matrix. This can be done knowing that any $M \times M$ submatrix of a unitary U, randomly chosen according to the Haar measure, is close in variation distance to a matrix of i.i.d. complex random Gaussian variables, provided that $M \leq N^{1/6}$ (Haar random matrices can be directly implemented in optical circuits by mapping independent probability density functions for their parameters, to optical circuit components, i.e., beam splitters and phase shifters[14]). Therefore, if the linear optical circuit implements a Haar random unitary matrix, the adversarial sampler will not be able to detect which of the exponentially many probabilities $p(t_1, t_2, \ldots, t_N)$ we care about, and thus will not be able to avoid its estimation. In this case $p(t_1, t_2, \ldots, t_N)$ is proportional to the squared absolute value of the permanent of the $M \times M$ matrix $X \sim \mathcal{N}(0,1)_{\mathcal{C}}^{M \times M}$ of i.i.d. Gaussians, smuggled inside U. These arguments bring us to the first conjecture of the hardness proof of approximate boson sampling problem – the permanent-of-Gaussians conjecture:

- Approximating the permanent of a matrix $X \sim \mathcal{N}(0,1)_{\mathcal{C}}^{M \times M}$ of i.i.d. Gaussians to within multiplicative error is a #P-hard task.

Moreover, the above conjecture can be linked to the estimation of $|\mathrm{Perm}\, X|^2$, which the given probability of a specific measurement outcome is proportional to. However to establish this link one has to rely on another conjecture – the permanent anticoncentration conjecture:

- There exists a polynomial Q such that for any M and $\delta > 0$ the probability over $M \times M$ matrices $X \sim \mathcal{N}(0,1)_{\mathcal{C}}^{M \times M}$ of the following inequality to hold is smaller than δ:

  $$|\mathrm{Perm}\, X| < \frac{\sqrt{M!}}{Q(M, 1/\delta)}.$$

By making use of the above two conjectures (which have several evidences of being true), the final proof eventually states that the existence of a classical polynomial-time algorithm for the approximate boson sampling task implies the collapse of the polynomial hierarchy. It is also worth mentioning another fact important to the proof of this statement, namely the so-called bosonic birthday paradox (in analogy with the well-known birthday paradox). The latter states that if M identical bosons are scattered among $N \gg M^2$ modes of a linear interferometer with no two bosons in the same mode, then with high probability two bosons will not be found in the same output mode either.[15] This property has been experimentally observed[16] with two and three photons in integrated interferometers of up to 16 modes. On the one hand this feature facilitates the implementation of a restricted boson sampling device. Namely, if the probability of having more than one photon at the output of a linear optical circuit is negligible, one does not require photon-number-resolving detectors anymore: on-off detectors will be sufficient for the realization of the setup.

Although the probability $p(t_1, t_2, \ldots, t_N)$ of a specific measurement outcome at the output of the interferometer is related to the permanent of submatrices of a unitary matrix, a boson sampling machine does not allow its estimation. The main reason behind is that the corresponding detection probability is usually exponentially small. Thus, in order to collect enough statistics to approximate its value, one has to run the quantum experiment for exponentially long time. Therefore, the estimate obtained from a boson sampler is not more efficient that running the classical polynomial-time algorithm by Gurvits for approximating the permanent of any matrix to within additive error.[17]

Variants

Scattershot boson sampling

As already mentioned above, for the implementation of a boson sampling machine one necessitates a reliable source of many indistinguishable photons, and this requirement currently remains one of the main difficulties in scaling up the complexity of the device. Namely, despite recent advances in photon generation techniques using atoms, molecules, quantum dots and color centers in diamonds, the most widely used method remains the parametric down-conversion (**PDC**) mechanism. The main advantages of PDC sources are the high photon indistinguishability, collection efficiency and relatively simple experimental setups. However, one of the drawbacks of this approach is its non-deterministic (heralded) nature. Specifically, suppose the probability of generating a single photon by means of a PDC crystal is ε. Then, the probability of generating simultaneously M single photons is ε^M, which decreases exponentially with M. In other words, in order to generate the input state for the boson sampling machine, one would have to wait for exponentially long time, which would kill the advantage of the quantum setup over a classical machine. Subsequently, this characteristic restricted the use of PDC sources to proof-of-principle demonstrations of a boson sampling device.

Recently, however, a new scheme has been proposed to make the best use of PDC sources for the needs of boson sampling, greatly enhancing the rate of M-photon events. This approach has been named **scattershot boson sampling**,[18][19] which consists of connecting N ($N>M$) heralded single-photon sources to different input ports of the linear interferometer. Then, by pumping all N PDC crystals with simultaneous laser pulses, the probability of generating M photons will be given as $\binom{N}{M}\varepsilon^M$. Therefore, for $N \gg M$, this results in an exponential improvement in the single photon generation rate with respect to the usual, fixed-input boson sampling with M sources. This setting can also be seen as a problem of sampling N two-mode squeezed vacuum states generated from N PDC sources.

Scattershot boson sampling is still intractable for a classical computer: in the conventional setup we fixed the columns that defined our $M \times M$ submatrix and only varied the rows, whereas now we vary the columns too, depending on which M out of N PDC crystals generated single photons. Therefore, the proof can be constructed here similar to the original one. Furthermore, scattershot boson sampling has been also recently implemented with six photon-pair sources coupled to integrated photonic circuits of nine and thirteen modes, being an important leap towards a convincing experimental demonstration of the quantum computational supremacy.[20] The scattershot boson sampling model can be further generalized to the case where both legs of PDC sources are subject to linear optical transformations (in the original

scattershot case, one of the arms is used for heralding, i.e., it goes through the identity channel). Such a **twofold** scattershot boson sampling model is also computationally hard, as proven by making use of the symmetry of quantum mechanics under time reversal.[21]

Gaussian boson sampling

Another photonic implementation of boson sampling concerns Gaussian input states, i.e. states whose quasiprobability Wigner distribution function is a Gaussian one. The hardness of the corresponding sampling task can be linked to that of scattershot boson sampling.[22] Namely, the latter can be embedded into the conventional boson sampling setup with Gaussian inputs. For this, one has to generate two-mode entangled Gaussian states and apply a Haar-random unitary U to their "right halves", while doing nothing to the others. Then we can measure the "left halves" to find out which of the input states contained a photon before we applied U. This is precisely equivalent to scattershot boson sampling, except for the fact that our measurement of the herald photons has been deferred till the end of the experiment, instead of happening at the beginning. Therefore, approximate Gaussian boson sampling can be argued to be hard under precisely the same complexity assumption as can approximate ordinary or scattershot boson sampling.[19] Gaussian resources can be employed at the measurement stage, as well. Namely, one can define a boson sampling model, where a linear optical evolution of input single-photon states is concluded by Gaussian measurements (more specifically, by eight-port homodyne detection that projects each output mode onto a squeezed coherent state). Such a model deals with continuous-variable measurement outcome, which, under certain conditions, is a computationally hard task.[21] Finally, a linear optics platform for implementing a boson sampling experiment where input single-photons undergo an active (non-linear) Gaussian transformation is also available. This setting makes use of a set of two-mode squeezed vacuum states as a prior resource, with no need of single-photon sources or in-line nonlinear amplification medium.[23] This variant uses the Hafnian, a generalization of the permanent.[22]

Classically simulable boson sampling tasks

The above results state that the existence of a polynomial-time classical algorithm for the original boson sampling scheme with indistinguishable single photons (in the exact and approximate cases), for scattershot, as well as for the general Gaussian boson sampling problems is highly unlikely. Nevertheless, there are some non-trivial realizations of the boson sampling problem that allow for its efficient classical simulation. One such example is when the optical circuit is injected with distinguishable single photons. In this case, instead of summing the probability *amplitudes* corresponding to photonic many-particle paths, one has to sum the corresponding probabilities (i.e. the squared absolute values of the amplitudes). Consequently, the detection probability $p(t_1, t_2, \ldots, t_N)$ will be proportional to the permanent of submatrices of (component-wise) squared absolute value of the unitary U. The latter is now a non-negative matrix. Therefore, although the exact computation of the corresponding permanent is a #P-complete problem, its approximation can be performed efficiently on a classical computer, due to the seminal algorithm by Jerrum, Sinclaire and Vigoda.[24] In other words, approximate boson sampling with distinguishable photons is efficiently classically simulable.

Another instance of classically simulable boson sampling setups consists of sampling from the probability distribution of coherent states injected into the linear interferometer. The reason is that at the output of a linear optical circuit coherent states remain such, and do not create any quantum entanglement among the modes. More precisely, only their amplitudes are transformed, and the transformation can be efficiently calculated on a classical computer (the computation comprises matrix multiplication). This fact

can be used to perform corresponding sampling tasks from another set of states: so-called classical states, whose Glauber-Sudarshan *P* function is a well-defined probability distribution. These states can be represented as a mixture of coherent states due to the optical equivalence theorem. Therefore, picking random coherent states distributed according to the corresponding *P* function, one can perform efficient classical simulation of boson sampling from this set of classical states.[25][26]

Experimental implementations

The above requirements for the photonic boson sampling machine allow for its small-scale construction by means of existing technologies. Consequently, shortly after the theoretical model was introduced, four different groups[3][4][6][7] simultaneously reported its realization.

Specifically, this included the implementation of boson sampling with:

- two and three photons scattered by a six-mode linear unitary transformation (represented by two orthogonal polarizations in 3×3 spatial modes of a fused-fiber beam splitter) by a collaboration between the University of Queensland and MIT[3]
- three photons in different modes of a six-mode silica-on-silicon waveguide circuit, by a collaboration between Universities of Oxford, Shanghai, London and Southampton[4]
- three photons in a femtosecond laser-written five-mode interferometer, by a collaboration between universities of Vienna and Jena[6]
- three photons in a femtosecond laser-written five-mode interferometer implementing a Haar-random unitary transformation, by a collaboration between Milan's Institute of Photonics and Nanotechnology, Universidade Federal Fluminense and Sapienza University of Rome.[7]

Later on, more complex boson sampling experiments have been performed, increasing the number of spatial modes of random interferometers up to 13[27] and 9[28] modes, and realizing a 6-mode fully reconfigurable integrated circuit.[8] These experiments altogether constitute the proof-of-principle demonstrations of an operational boson sampling device, and route towards its larger-scale implementations.

Implementation of scattershot boson sampling

A first scattershot boson sampling experiment has been recently implemented[20] using six photon-pair sources coupled to integrated photonic circuits with 13 modes. The 6 photon-pair sources were obtained via type-II PDC processes in 3 different nonlinear crystals (exploiting the polarization degree of freedom). This allowed to sample simultaneously between 8 different input states. The 13-mode interferometer was realized by femtosecond laser-writing technique on alumino-borosilicate glas.

This experimental implementation represents a leap towards an experimental demonstration of the quantum computational supremacy.[20]

Proposals with alternative photonic platform

There are several other proposals for the implementation of photonic boson sampling. This includes, e.g., the scheme for arbitrarily scalable boson sampling using two nested fiber loops. In this case, the architecture employs time-bin encoding, whereby the incident photons form a pulse train entering the

loops. Meanwhile, dynamically controlled loop coupling ratios allow the construction of arbitrary linear interferometers. Moreover, the architecture employs only a single point of interference and may thus be easier to stabilize than other implementations.[29]

Another approach relies on the realization of unitary transformations on temporal modes based on dispersion and pulse shaping. Namely, passing consecutively heralded photons through time-independent dispersion and measuring the output time of the photons is equivalent to a boson sampling experiment. With time-dependent dispersion, it is also possible to implement arbitrary single-particle unitaries. This scheme requires a much smaller number of sources and detectors and do not necessitate a large system of beam splitters.[30]

Certification

The output of a universal quantum computer running, for example, Shor's factoring algorithm, can be efficiently verified classically, as is the case for all problems in the non-deterministic polynomial-time (NP) complexity class. It is however not clear that a similar structure exists for the boson sampling scheme. Namely, as the latter is related to the problem of estimating matrix permanents (falling into #P-hard complexity class), it is not understood how to verify correct operation for large versions of the setup. Specifically, the naive verification of the output of a boson sampler by computing the corresponding measurement probabilities represents a problem intractable for a classical computer.

A first relevant question is whether it is possible or not to distinguish between uniform and boson-sampling distributions by performing a polynomial number of measurements. The initial argument introduced in Ref.[31] stated that as long as one makes use of symmetric measurement settings the above is impossible (roughly speaking a symmetric measurement scheme does not allow for labeling the output modes of the optical circuit). However, within current technologies the assumption of a symmetric setting is not justified (the tracking of the measurement statistics is fully accessible), and therefore the above argument does not apply. It is then possible to define a rigorous and efficient test to discriminate the boson sampling statistics from an unbiased probability distribution.[32] The corresponding discriminator is correlated to the permanent of the submatrix associated with a given measurement pattern, but can be efficiently calculated. This test has been applied experimentally to distinguish between a boson sampling and a uniform distribution in the 3-photon regime with integrated circuits of 5, 7, 9[28] and 13 modes.[27]

The test above does not distinguish between more complex distributions, such as quantum and classical, or between fermionic and bosonic statistics. A physically motivated scenario to be addressed is the unwanted introduction of distinguishability between photons, which destroys quantum interference (this regime is readily accessible experimentally, for example by introducing temporal delay between photons). The opportunity then exists to tune between ideally indistinguishable (quantum) and perfectly distinguishable (classical) data and measure the change in a suitably constructed metric. This scenario can be addressed by a statistical test which performs a one-on-one likelihood comparison of the output probabilities. This test requires the calculation of a small number of permanents, but does not need the calculation of the full expected probability distribution. Experimental implementation of the test has been successfully reported in integrated laser-written circuits for both the standard boson sampling[27] (3 photons in 7-, 9- and 13-mode interferometers) and the scattershot version[20] (3 photons in 9- and 13-mode interferometers with different input states). Another possibility is based on the bunching property of indinguishable photons. One can analyze the probability to find a *k*-fold coincidence measurement

outcomes (without any multiply populated input mode), which is significantly higher for distinguishable particles than for bosons due to the bunching tendency of the latters.[28] Finally, leaving the space of random matrices one may focus on specific multimode setups with certain features. In particular, the analysis of the effect of bosonic clouding (the tendency for bosons to favor events with all particles in the same half of the output array of a continuous-time many-particle quantum walk) has been proven to discriminate the behavior of distinguishable and indistinguishable particles in this specific platform.[28]

A different approach to confirm that the boson sampling machine behaves as the theory predicts is to make use of fully reconfigurable optical circuits. With large-scale single-photon and multiphoton interference verified with predictable multimode correlations in a fully characterized circuit, a reasonable assumption is that the system maintains correct operation as the circuit is continuously reconfigured to implement a random unitary operation. To this end, one can exploit quantum suppression laws (the probability of specific input-output combinations is suppressed when the linear interferometer is described by a Fourier matrix or other matrices with relevant symmetries).[33] These suppression laws can be classically predicted in efficient ways. This approach allows also to exclude other physical models, such as mean-field states, which mimic some collective multiparticle properties (including bosonic clouding). The implementation of a Fourier matrix circuit in a fully reconfigurable 6-mode device has been reported,[8] and experimental observations of the suppression law have been shown for 2 photons in 4- and 8-mode Fourier matrices.[34]

Alternative implementations and applications

Apart from the photonic realization of the boson sampling task, several other setups have been proposed. This includes, e.g., the encoding of bosons into the local transverse phonon modes of trapped ions. The scheme allows deterministic preparation and high-efficiency readout of the corresponding phonon Fock states and universal manipulation of the phonon modes through a combination of inherent Coulomb interaction and individual phase shifts.[35] This scheme is scalable and relies on the recent advances in ion trapping techniques (several dozens of ions can be successfully trapped, for example, in linear Paul traps by making use of anharmonic axial potentials).

Another platform for implementing the boson sampling setup is a system of interacting spins: recent observation show that boson sampling with M particles in N modes is equivalent to the short-time evolution with M excitations in the XY model of $2N$ spins.[36] One necessitates several additional assumptions here, including small boson bunching probability and efficient error postselection. This scalable scheme, however, is rather promising, in the light of considerable development in the construction and manipulation of coupled superconducting qubits and specifically the D-Wave machine.

The task of boson sampling shares peculiar similarities with the problem of determining molecular vibronic spectra: a feasible modification of the boson sampling scheme results in a setup that can be used for the reconstruction of a molecule's Franck–Condon profiles (for which no efficient classical algorithm is currently known). Specifically, the task now is to input specific squeezed coherent states into a linear interferometer that is determined by the properties of the molecule of interest.[37] Therefore, this prominent observation makes the interest towards the implementation of the boson sampling task to get spread well beyond the fundamental basis.

It has also been suggested to use a superconducting resonator network Boson Sampling device as an interferometer. This application is assumed to be practical, as small changes in the couplings between the resonators will change the sampling results. Sensing of variation in the parameters capable of altering the couplings is thus achieved, when comparing the sampling results to an unaltered reference.[38]

Variants of the boson sampling model have been used to construct *classical* computational algorithms, aimed, e.g., at the estimation of certain matrix permanents (for instance, permanents of positive-semidefinite matrices related to the corresponding open problem in computer science[39]) by combining tools proper to quantum optics and computational complexity.[40]

Coarse-grained boson sampling has been proposed as a resource of decision and function problems that are computationally hard, and may thus have cryptographic applications.[41][42][43] The first related proof-of-principle experiment was performed with a photonic boson-sampling machine (fabricated by a direct femtosecond laser-writing technique),[44] and confirmed many of the theoretical predictions.

Gaussian boson sampling has been analyzed as a search component for computing binding propensity between molecules of pharmacological interest as well.[45]

See also

- Quantum random circuits
- Cross-entropy benchmarking
- Linear optical quantum computing
- KLM protocol

References

1. Aaronson, Scott; Arkhipov, Alex (2013). "The computational complexity of linear optics" (https://doi.org/10.4086%2Ftoc.2013.v009a004). *Theory of Computing*. **9**: 143–252. doi:10.4086/toc.2013.v009a004 (https://doi.org/10.4086%2Ftoc.2013.v009a004).
2. Troyansky, Lidror; Tishby, Naftali (1996). “Permanent uncertainty: On the quantum evaluation of the determinant and the permanent of a matrix”. Proceedings of PhysComp, 1996: 314-318.
3. Broome, Matthew; Fedrizzi, Alessandro; Rahimi-Keshari, Saleh; Dove, Justin; Aaronson, Scott; Ralph, Timothy; White, Andrew (2013). "Photonic boson sampling in a tunable circuit". *Science*. **339** (6121): 794–798. arXiv:1212.2234 (https://arxiv.org/abs/1212.2234). Bibcode:2013Sci...339..794B (https://ui.adsabs.harvard.edu/abs/2013Sci...339..794B). doi:10.1126/science.1231440 (https://doi.org/10.1126%2Fscience.1231440). PMID 23258411 (https://pubmed.ncbi.nlm.nih.gov/23258411). S2CID 22912771 (https://api.semanticscholar.org/CorpusID:22912771).
4. Spring, Justin; Metcalf, Benjamin; Humphreys, Peter; Kolthammer, Steven; Jin, Xian-Min; Barbieri, Marco; Datta, Animesh; Thomas-Peter, Nicholas; Langford, Nathan; Kundys, Dmytro; Gates, James; Smith, Brian; Smith, Peter; Walmsley, Ian (2013). "Boson sampling on a photonic chip". *Science*. **339** (6121): 798–801. arXiv:1212.2622 (https://arxiv.org/abs/1212.2622). Bibcode:2013Sci...339..798S (https://ui.adsabs.harvard.edu/abs/2013Sci...339..798S). doi:10.1126/science.1231692 (https://doi.org/10.1126%2Fscience.1231692). PMID 23258407 (https://pubmed.ncbi.nlm.nih.gov/23258407). S2CID 11687876 (https://api.semanticscholar.org/CorpusID:11687876).

5. Szameit, Alexander; Dreisow, Felix; Pertsch, Thomas; Nolte, Stefan; Tünnermann, Andreas (2007). "Control of directional evanescent coupling in fs laser written waveguides" (https://doi.org/10.1364%2FOE.15.001579). *Optics Express*. **15** (4): 1579–1587. Bibcode:2007OExpr..15.1579S (https://ui.adsabs.harvard.edu/abs/2007OExpr..15.1579S). doi:10.1364/OE.15.001579 (https://doi.org/10.1364%2FOE.15.001579). PMID 19532390 (https://pubmed.ncbi.nlm.nih.gov/19532390).
6. Tillmann, Max; Dakic, Borivoje; Heilmann, Rene; Nolte, Stefan; Szameit, Alexander; Walther, Philip (2013). "Experimental boson sampling". *Nature Photonics*. **7** (7): 540–544. arXiv:1212.2240 (https://arxiv.org/abs/1212.2240). Bibcode:2013NaPho...7..540T (https://ui.adsabs.harvard.edu/abs/2013NaPho...7..540T). doi:10.1038/nphoton.2013.102 (https://doi.org/10.1038%2Fnphoton.2013.102). S2CID 119241050 (https://api.semanticscholar.org/CorpusID:119241050).
7. Crespi, Andrea; Osellame, Roberto; Ramponi, Roberta; Brod, Daniel; Galvao, Ernesto; Spagnolo, Nicolò; Vitelli, Chiara; Maiorino, Enrico; Mataloni, Paolo; Sciarrino, Fabio (2013). "Integrated multimode interferometers with arbitrary designs for photonic boson sampling". *Nature Photonics*. **7** (7): 545–549. arXiv:1212.2783 (https://arxiv.org/abs/1212.2783). Bibcode:2013NaPho...7..545C (https://ui.adsabs.harvard.edu/abs/2013NaPho...7..545C). doi:10.1038/nphoton.2013.112 (https://doi.org/10.1038%2Fnphoton.2013.112). S2CID 121093296 (https://api.semanticscholar.org/CorpusID:121093296).
8. Carolan, Jacques; Harrold, Christopher; Sparrow, Chris; et al. (2015). "Universal linear optics". *Science*. **349** (6249): 711–716. arXiv:1505.01182 (https://arxiv.org/abs/1505.01182). doi:10.1126/science.aab3642 (https://doi.org/10.1126%2Fscience.aab3642). PMID 26160375 (https://pubmed.ncbi.nlm.nih.gov/26160375). S2CID 19067232 (https://api.semanticscholar.org/CorpusID:19067232).
9. Scheel, Stefan (2008). "Permanents in linear optical networks". *Acta Physica Slovaca*. **58** (5): 675. arXiv:quant-ph/0406127 (https://arxiv.org/abs/quant-ph/0406127). Bibcode:2004quant.ph..6127S (https://ui.adsabs.harvard.edu/abs/2004quant.ph..6127S). doi:10.2478/v10155-010-0092-x (https://doi.org/10.2478%2Fv10155-010-0092-x). S2CID 121606171 (https://api.semanticscholar.org/CorpusID:121606171).
10. "Polynomial-time hierarchy" (https://archive.today/20140214114948/https://complexityzoo.uwaterloo.ca/). *Complexity Zoo*. Archived from the original (https://complexityzoo.uwaterloo.ca) on February 14, 2014.
11. Bremner, Michael; Jozsa, Richard; Shepherd, Dan (2011). "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy". *Proc. R. Soc. A*. **467** (2126): 459–472. arXiv:1005.1407 (https://arxiv.org/abs/1005.1407). Bibcode:2011RSPSA.467..459B (https://ui.adsabs.harvard.edu/abs/2011RSPSA.467..459B). doi:10.1098/rspa.2010.0301 (https://doi.org/10.1098%2Frspa.2010.0301). S2CID 12301677 (https://api.semanticscholar.org/CorpusID:12301677).
12. Aaronson, Scott (2005). "Quantum computing, postselection, and probabilistic polynomial-time". *Proc. R. Soc. A*. **461** (2063): 3473–3482. arXiv:quant-ph/0412187 (https://arxiv.org/abs/quant-ph/0412187). Bibcode:2005RSPSA.461.3473A (https://ui.adsabs.harvard.edu/abs/2005RSPSA.461.3473A). doi:10.1098/rspa.2005.1546 (https://doi.org/10.1098%2Frspa.2005.1546). S2CID 1770389 (https://api.semanticscholar.org/CorpusID:1770389).
13. Clifford, Peter; Clifford, Raphaël (2017-06-05). "The Classical Complexity of Boson Sampling". arXiv:1706.01260 (https://arxiv.org/abs/1706.01260) [cs.DS (https://arxiv.org/archive/cs.DS)].
14. Russell, Nicholas; Chakhmakhchyan, Levon; O'Brien, Jeremy; Laing, Anthony (2017). "Direct dialling of Haar random unitary matrices". *New J. Phys*. **19** (3): 033007. arXiv:1506.06220 (https://arxiv.org/abs/1506.06220). Bibcode:2017NJPh...19c3007R (https://ui.adsabs.harvard.edu/abs/2017NJPh...19c3007R). doi:10.1088/1367-2630/aa60ed (https://doi.org/10.1088%2F1367-2630%2Faa60ed). S2CID 46915633 (https://api.semanticscholar.org/CorpusID:46915633).

15. Arkhipov, Alex; Kuperberg, Greg (2012). "The bosonic birthday paradox". *Geometry & Topology Monographs*. Proceedings of the Freedman Fest. **18**: 1–7. arXiv:1106.0849 (https://arxiv.org/abs/1106.0849). doi:10.2140/gtm.2012.18.1 (https://doi.org/10.2140%2Fgtm.2012.18.1). S2CID 41510747 (https://api.semanticscholar.org/CorpusID:41510747).
16. Spagnolo, Nicolò; Vitelli, Chiara; Sanson, Linda; et al. (2013). "General Rules for Bosonic Bunching in Multimode Interferometers". *Phys. Rev. Lett*. **111** (13): 130503. arXiv:1305.3188 (https://arxiv.org/abs/1305.3188). Bibcode:2013PhRvL.111m0503S (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111m0503S). doi:10.1103/PhysRevLett.111.130503 (https://doi.org/10.1103%2FPhysRevLett.111.130503). PMID 24116759 (https://pubmed.ncbi.nlm.nih.gov/24116759). S2CID 26984278 (https://api.semanticscholar.org/CorpusID:26984278).
17. Gurvits, Leonid (2005). "On the complexity of mixed discriminants and related problems". *Mathematical Foundations of Computer Science*: 447–458.
18. Lund, Austin; Laing, Anthony; Rahimi-Keshari, Saleh; et al. (2014). "Boson sampling from a Gaussian state". *Phys. Rev. Lett*. **113** (10): 100502. arXiv:1305.4346 (https://arxiv.org/abs/1305.4346). Bibcode:2014PhRvL.113j0502L (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113j0502L). doi:10.1103/PhysRevLett.113.100502 (https://doi.org/10.1103%2FPhysRevLett.113.100502). PMID 25238340 (https://pubmed.ncbi.nlm.nih.gov/25238340). S2CID 27742471 (https://api.semanticscholar.org/CorpusID:27742471).
19. Aaronson, Scott (8 November 2013). "Scattershot BosonSampling: a new approach to scalable BosonSampling experiments" (http://www.scottaaronson.com/blog/?p=1579). *Shtetl-Optimized*.
20. Bentivegna, Marco; Spagnolo, Nicolo; Vitelli, Chiara; Flamini, Fulvio; Viggianiello, Niko; Latmiral, Ludovico; Mataloni, Paolo; Brod, Daniel; Galvão, Ernesto; Crespi, Andrea; Ramponi, Roberta; Osellame, Roberto; Sciarrino, Fabio (2015). "Experimental scattershot boson sampling" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4640628). *Science Advances*. **1** (3): e1400255. arXiv:1505.03708 (https://arxiv.org/abs/1505.03708). Bibcode:2015SciA....1E0255B (https://ui.adsabs.harvard.edu/abs/2015SciA....1E0255B). doi:10.1126/sciadv.1400255 (https://doi.org/10.1126%2Fsciadv.1400255). PMC 4640628 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4640628). PMID 26601164 (https://pubmed.ncbi.nlm.nih.gov/26601164).
21. Chakhmakhchyan, Levon; Cerf, Nicolas (2017). "Boson sampling with Gaussian measurements". *Phys. Rev. A*. **96** (3): 032326. arXiv:1705.05299 (https://arxiv.org/abs/1705.05299). Bibcode:2017PhRvA..96c2326C (https://ui.adsabs.harvard.edu/abs/2017PhRvA..96c2326C). doi:10.1103/PhysRevA.96.032326 (https://doi.org/10.1103%2FPhysRevA.96.032326). S2CID 119431211 (https://api.semanticscholar.org/CorpusID:119431211).
22. Hamilton, Craig S.; Kruse, Regina; Sansoni, Linda; Barkhofen, Sonja; Silberhorn, Christine; Jex, Igor (23 October 2017). "Gaussian Boson Sampling" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.119.170501). *Physical Review Letters*. **119** (17): 170501. arXiv:1612.01199 (https://arxiv.org/abs/1612.01199). Bibcode:2017PhRvL.119q0501H (https://ui.adsabs.harvard.edu/abs/2017PhRvL.119q0501H). doi:10.1103/PhysRevLett.119.170501 (https://doi.org/10.1103%2FPhysRevLett.119.170501). PMID 29219463 (https://pubmed.ncbi.nlm.nih.gov/29219463). S2CID 1665615 (https://api.semanticscholar.org/CorpusID:1665615). Retrieved 22 January 2021.
23. Chakhmakhchyan, Levon; Cerf, Nicolas (2018). "Simulating arbitrary Gaussian circuits with linear optics". *Phys. Rev. A*. **98** (6): 062314. arXiv:1803.11534 (https://arxiv.org/abs/1803.11534). Bibcode:2018PhRvA..98f2314C (https://ui.adsabs.harvard.edu/abs/2018PhRvA..98f2314C). doi:10.1103/PhysRevA.98.062314 (https://doi.org/10.1103%2FPhysRevA.98.062314). S2CID 119227039 (https://api.semanticscholar.org/CorpusID:119227039).
24. Jerrum, Mark; Sinclair, Alistair; Vigoda, Eric (2001). "A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries". *Journal of the ACM*. **51** (4): 671–697. CiteSeerX 10.1.1.18.9466 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.18.9466). doi:10.1145/1008731.1008738 (https://doi.org/10.1145%2F1008731.1008738). S2CID 47361920 (https://api.semanticscholar.org/CorpusID:47361920).

25. Rahimi-Keshari, Saleh; Lund, Austin; Ralph, Timothy (2015). "What can quantum optics say about computational complexity theory?". *Phys. Rev. Lett*. **114** (6): 060501. arXiv:1408.3712 (https://arxiv.org/abs/1408.3712). Bibcode:2015PhRvL.114f0501R (https://ui.adsabs.harvard.edu/abs/2015PhRvL.114f0501R). doi:10.1103/PhysRevLett.114.060501 (https://doi.org/10.1103%2FPhysRevLett.114.060501). PMID 25723196 (https://pubmed.ncbi.nlm.nih.gov/25723196). S2CID 436866 (https://api.semanticscholar.org/CorpusID:436866).
26. Rahimi-Keshari, Saleh; Ralph, Timothy; Carlton, Caves (2016). "Efficient classical simulation of quantum optics". *Physical Review X*. **6** (2): 021039. arXiv:1511.06526 (https://arxiv.org/abs/1511.06526). Bibcode:2016PhRvX...6b1039R (https://ui.adsabs.harvard.edu/abs/2016PhRvX...6b1039R). doi:10.1103/PhysRevX.6.021039 (https://doi.org/10.1103%2FPhysRevX.6.021039). S2CID 23490704 (https://api.semanticscholar.org/CorpusID:23490704).
27. Spagnolo, Nicolo; Vitelli, Chiara; Bentivegna, Marco; Brod, Daniel; Crespi, Andrea; Flamini, Fulvio; Giacomini, Sandro; Milani, Giorgio; Ramponi, Roberta; Mataloni, Paolo; Osellame, Roberto; Galvão, Ernesto; Sciarrino, Fabio (2014). "Experimental validation of photonic boson sampling". *Nature Photonics*. **8** (8): 615–620. arXiv:1311.1622 (https://arxiv.org/abs/1311.1622). Bibcode:2014NaPho...8..615S (https://ui.adsabs.harvard.edu/abs/2014NaPho...8..615S). doi:10.1038/nphoton.2014.135 (https://doi.org/10.1038%2Fnphoton.2014.135). S2CID 120825561 (https://api.semanticscholar.org/CorpusID:120825561).
28. Carolan, Jacques; Meinecke, Jasmin; Shadbolt, Pete; Russell, Nicholas; Ismail, Nur; Wörhoff, Kerstin; Rudolph, Terry; Thompson, Mark; O'Brien, Jeremy; Matthews, Jonathan; Laing, Anthony (2014). "On the experimental verification of quantum complexity in linear optics". *Nature Photonics*. **8** (8): 621–626. arXiv:1311.2913 (https://arxiv.org/abs/1311.2913). Bibcode:2014NaPho...8..621C (https://ui.adsabs.harvard.edu/abs/2014NaPho...8..621C). doi:10.1038/nphoton.2014.152 (https://doi.org/10.1038%2Fnphoton.2014.152). S2CID 10874278 (https://api.semanticscholar.org/CorpusID:10874278).
29. Motes, Keith; Gilchrist, Alexei; Dowling, Jonathan; Rohde, Peter (2014). "Scalable boson sampling with time-bin encoding using a loop-based architecture". *Phys. Rev. Lett*. **113** (12): 120501. arXiv:1403.4007 (https://arxiv.org/abs/1403.4007). Bibcode:2014PhRvL.113l0501M (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113l0501M). doi:10.1103/PhysRevLett.113.120501 (https://doi.org/10.1103%2FPhysRevLett.113.120501). PMID 25279613 (https://pubmed.ncbi.nlm.nih.gov/25279613). S2CID 33602886 (https://api.semanticscholar.org/CorpusID:33602886).
30. Pant, Mihir; Englund, Dirk (2016). "High dimensional unitary transformations and boson sampling on temporal modes using dispersive optics". *Physical Review A*. **93** (4): 043803. arXiv:1505.03103 (https://arxiv.org/abs/1505.03103). Bibcode:2016PhRvA..93d3803P (https://ui.adsabs.harvard.edu/abs/2016PhRvA..93d3803P). doi:10.1103/PhysRevA.93.043803 (https://doi.org/10.1103%2FPhysRevA.93.043803). S2CID 5022049 (https://api.semanticscholar.org/CorpusID:5022049).
31. Gogolin, C.; Kliesch, M.; Aolita, L.; Eisert, J. (2013). "Boson-Sampling in the light of sample complexity". arXiv:1306.3995 (https://arxiv.org/abs/1306.3995) [quant-ph (https://arxiv.org/archive/quant-ph)].
32. Aaronson, Scott; Arkhipov, Alex (2013). "BosonSampling is far from uniform". arXiv:1309.7460 (https://arxiv.org/abs/1309.7460) [quant-ph (https://arxiv.org/archive/quant-ph)].
33. Tichy, Malte; Mayer, Klaus; Buchleitner, Andreas; Mølmer, Klaus (2014). "Stringent and Efficient Assessment of Boson-Sampling Devices". *Phys. Rev. Lett*. **113** (2): 020502. arXiv:1312.3080 (https://arxiv.org/abs/1312.3080). Bibcode:2014PhRvL.113b0502T (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113b0502T). doi:10.1103/PhysRevLett.113.020502 (https://doi.org/10.1103%2FPhysRevLett.113.020502). PMID 25062152 (https://pubmed.ncbi.nlm.nih.gov/25062152). S2CID 44653164 (https://api.semanticscholar.org/CorpusID:44653164).

34. Crespi, Andrea; Osellame, Roberto; Ramponi, Roberta; et al. (2016). "Quantum suppression law in a 3-D photonic chip implementing the fast Fourier transform" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4742850). *Nature Communications*. **7**: 10469. arXiv:1508.00782 (https://arxiv.org/abs/1508.00782). Bibcode:2015arXiv150800782C (https://ui.adsabs.harvard.edu/abs/2015arXiv150800782C). doi:10.1038/ncomms10469 (https://doi.org/10.1038%2Fncomms10469). PMC 4742850 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4742850). PMID 26843135 (https://pubmed.ncbi.nlm.nih.gov/26843135).
35. Shen, C.; Zhang, Z.; Duan, L.-M. (2014). "Scalable implementation of boson sampling with trapped ions". *Phys. Rev. Lett*. **112** (5): 050504. arXiv:1310.4860 (https://arxiv.org/abs/1310.4860). Bibcode:2014PhRvL.112e0504S (https://ui.adsabs.harvard.edu/abs/2014PhRvL.112e0504S). doi:10.1103/PhysRevLett.112.050504 (https://doi.org/10.1103%2FPhysRevLett.112.050504). PMID 24580579 (https://pubmed.ncbi.nlm.nih.gov/24580579). S2CID 10489988 (https://api.semanticscholar.org/CorpusID:10489988).
36. Peropadre, Borja; Aspuru-Guzik, Alan; Garcia-Ripoll, Juan (2015). "Spin models and boson sampling". arXiv:1509.02703 (https://arxiv.org/abs/1509.02703) [quant-ph (https://arxiv.org/archive/quant-ph)].
37. Huh, Joonsuk; Giacomo Guerreschi, Gian; Peropadre, Borja; McClean, Jarrod; Aspuru-Guzik, Alan (2015). "Boson sampling for molecular vibronic spectra". *Nature Photonics*. **9** (9): 615–620. arXiv:1412.8427 (https://arxiv.org/abs/1412.8427). Bibcode:2015NaPho...9..615H (https://ui.adsabs.harvard.edu/abs/2015NaPho...9..615H). doi:10.1038/NPHOTON.2015.153 (https://doi.org/10.1038%2FNPHOTON.2015.153). S2CID 960357 (https://api.semanticscholar.org/CorpusID:960357).
38. Goldstein, Samuel; Korenblit, Simcha; Bendor, Ydan; You, Hao; Geller, Michael R.; Katz, Nadav (17 January 2017). "Decoherence and interferometric sensitivity of boson sampling in superconducting resonator networks". *Phys. Rev. B*. **95** (2): 020502. arXiv:1701.00714 (https://arxiv.org/abs/1701.00714). Bibcode:2017PhRvB..95b0502G (https://ui.adsabs.harvard.edu/abs/2017PhRvB..95b0502G). doi:10.1103/PhysRevB.95.020502 (https://doi.org/10.1103%2FPhysRevB.95.020502). S2CID 119077553 (https://api.semanticscholar.org/CorpusID:119077553).
39. See open problem (4) at "Shtetl Optimized: Introducing some British people to P vs. NP" (http://www.scottaaronson.com/blog/?p=2408#comment-757410). 22 July 2015.
40. Chakhmakhchyan, Levon; Cerf, Nicolas; Garcia-Patron, Raul (2017). "A quantum-inspired algorithm for estimating the permanent of positive semidefinite matrices". *Phys. Rev. A*. **96** (2): 022329. arXiv:1609.02416 (https://arxiv.org/abs/1609.02416). Bibcode:2017PhRvA..96b2329C (https://ui.adsabs.harvard.edu/abs/2017PhRvA..96b2329C). doi:10.1103/PhysRevA.96.022329 (https://doi.org/10.1103%2FPhysRevA.96.022329). S2CID 54194194 (https://api.semanticscholar.org/CorpusID:54194194).
41. Nikolopoulos, Georgios M.; Brougham, Thomas (2016). "Decision and function problems based on boson sampling". *Physical Review A*. **94** (1): 012315. arXiv:1607.02987 (https://arxiv.org/abs/1607.02987). Bibcode:2016PhRvA..94a2315N (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94a2315N). doi:10.1103/PhysRevA.94.012315 (https://doi.org/10.1103%2FPhysRevA.94.012315). S2CID 5311008 (https://api.semanticscholar.org/CorpusID:5311008).
42. Nikolopoulos, Georgios M. (2019). "Cryptographic one-way function based on boson sampling". *Quantum Information Processing*. **18** (8): 259. arXiv:1607.02987 (https://arxiv.org/abs/1607.02987). Bibcode:2019QuIP...18..259N (https://ui.adsabs.harvard.edu/abs/2019QuIP...18..259N). doi:10.1007/s11128-019-2372-9 (https://doi.org/10.1007%2Fs11128-019-2372-9). S2CID 195791867 (https://api.semanticscholar.org/CorpusID:195791867).
43. Nikolopoulos, Georgios M (2022-11-29). "Computational indistinguishability and boson sampling*" (https://doi.org/10.1088%2F1402-4896%2Faca1ed). *Physica Scripta*. **98** (1): 014001. arXiv:2211.04420 (https://arxiv.org/abs/2211.04420). doi:10.1088/1402-4896/aca1ed (https://doi.org/10.1088%2F1402-4896%2Faca1ed). ISSN 0031-8949 (https://search.worldcat.org/issn/0031-8949).

44. Wang, Xiao-Wei; Zhou, Wen-Hao; Fu, Yu-Xuan; Gao, Jun; Lu, Yong-Heng; Chang, Yi-Jun; Qiao, Lu-Feng; Ren, Ruo-Jing; Jiang, Ze-Kun; Jiao, Zhi-Qiang; Nikolopoulos, Georgios M.; Jin, Xian-Min (2023-02-09). "Experimental Boson Sampling Enabling Cryptographic One-Way Function" (https://link.aps.org/doi/10.1103/PhysRevLett.130.060802). *Physical Review Letters*. **130** (6): 060802. Bibcode:2023PhRvL.130f0802W (https://ui.adsabs.harvard.edu/abs/2023PhRvL.130f0802W). doi:10.1103/PhysRevLett.130.060802 (https://doi.org/10.1103%2FPhysRevLett.130.060802). PMID 36827576 (https://pubmed.ncbi.nlm.nih.gov/36827576). S2CID 256757275 (https://api.semanticscholar.org/CorpusID:256757275).
45. Banchi, Leonardo; Fingerhuth, Mark; Babej, Tomas; Ing, Christopher; Arrazola, Juan Miguel (2020). "Molecular docking with Gaussian Boson Sampling" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7274809). *Science Advances*. **6** (23): eaax1950. arXiv:1902.00462 (https://arxiv.org/abs/1902.00462). Bibcode:2020SciA....6.1950B (https://ui.adsabs.harvard.edu/abs/2020SciA....6.1950B). doi:10.1126/sciadv.aax1950 (https://doi.org/10.1126%2Fsciadv.aax1950). PMC 7274809 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7274809). PMID 32548251 (https://pubmed.ncbi.nlm.nih.gov/32548251).

External links

- QUCHIP project (http://www.quchip.eu)
- Quantum Information Lab – Sapienza: video on boson sampling (https://www.youtube.com/watch?v=jiodj5b8Z1E)
- Quantum Information Lab – Sapienza: video on scattershot boson sampling (https://www.youtube.com/watch?v=VPChHtm5ifs)
- The Qubit Lab – Boson Sampling (https://www.youtube.com/watch?v=Y2twOkiMRh0)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Boson_sampling&oldid=1193533400"

WIKIPEDIA
The Free Encyclopedia

Deutsch–Jozsa algorithm

The **Deutsch–Jozsa algorithm** is a deterministic quantum algorithm proposed by David Deutsch and Richard Jozsa in 1992 with improvements by Richard Cleve, Artur Ekert, Chiara Macchiavello, and Michele Mosca in 1998.[1][2] Although of little practical use, it is one of the first examples of a quantum algorithm that is exponentially faster than any possible deterministic classical algorithm.[3]

The Deutsch–Jozsa problem is specifically designed to be easy for a quantum algorithm and hard for any deterministic classical algorithm. It is a black box problem that can be solved efficiently by a quantum computer with no error, whereas a deterministic classical computer would need a exponential number of queries to the black box to solve the problem. More formally, it yields an oracle relative to which **EQP**, the class of problems that can be solved exactly in polynomial time on a quantum computer, and **P** are different.[4]

Since the problem is easy to solve on a probabilistic classical computer, it does not yield an oracle separation with **BPP**, the class of problems that can be solved with bounded error in polynomial time on a probabilistic classical computer. Simon's problem is an example of a problem that yields an oracle separation between **BQP** and **BPP**.

Problem statement

In the Deutsch–Jozsa problem, we are given a black box quantum computer known as an oracle that implements some function:

$$f: \{0,1\}^n \to \{0,1\}$$

The function takes n-bit binary values as input and produces either a 0 or a 1 as output for each such value. We are promised that the function is either constant (0 on all inputs or 1 on all inputs) or *balanced* (1 for exactly half of the input domain and 0 for the other half).[1] The task then is to determine if f is constant or balanced by using the oracle.

Classical solution

For a conventional deterministic algorithm where n is the number of bits, $2^{n-1}+1$ evaluations of f will be required in the worst case. To prove that f is constant, just over half the set of inputs must be evaluated and their outputs found to be identical (because the function is guaranteed to be either balanced or constant, not somewhere in between). The best case occurs where the function is balanced and the first two output values are different. For a conventional randomized algorithm, a constant k evaluations of the function suffices to produce the correct answer with a high probability (failing with probability $\epsilon \leq 1/2^k$

with $k \geq 1$). However, $k = 2^{n-1} + 1$ evaluations are still required if we want an answer that has no possibility of error. The Deutsch-Jozsa quantum algorithm produces an answer that is always correct with a single evaluation of f.

History

The Deutsch–Jozsa algorithm generalizes earlier (1985) work by David Deutsch, which provided a solution for the simple case where $n = 1$.
Specifically, given a Boolean function whose input is one bit, $f : \{0,1\} \to \{0,1\}$, is it constant?[5]

The algorithm, as Deutsch had originally proposed it, was not deterministic. The algorithm was successful with a probability of one half. In 1992, Deutsch and Jozsa produced a deterministic algorithm which was generalized to a function which takes n bits for its input. Unlike Deutsch's algorithm, this algorithm required two function evaluations instead of only one.

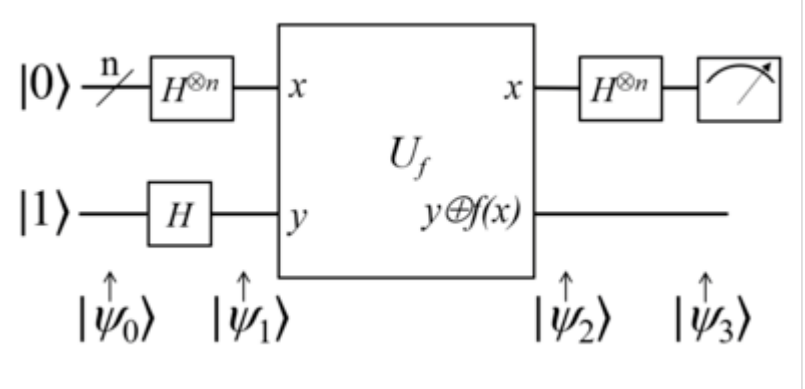
Further improvements to the Deutsch–Jozsa algorithm were made by Cleve et al.,[2] resulting in an algorithm that is both deterministic and requires only a single query of f. This algorithm is still referred to as Deutsch–Jozsa algorithm in honour of the groundbreaking techniques they employed.[2]

Algorithm

For the Deutsch–Jozsa algorithm to work, the oracle computing $f(x)$ from x must be a quantum oracle which does not decohere x. It also must not make a copy of x, because that would violate the no cloning theorem.

The algorithm begins with the $n + 1$ bit state $|0\rangle^{\otimes n}|1\rangle$. That is, the first n bits are each in the state $|0\rangle$ and the final bit is $|1\rangle$. A Hadamard gate is applied to each bit to obtain the state

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle),$$



Deutsch-Jozsa algorithm quantum circuit

where x runs over all n-bit strings. We have the function f implemented as a quantum oracle. The oracle maps its input state $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$, where $\oplus$ denotes addition modulo 2. Applying the quantum oracle gives;

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle).$$

For each x, $f(x)$ is either 0 or 1. Testing these two possibilities, we see the above state is equal to

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle).$$

At this point the last qubit $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ may be ignored and the following remains:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle.$$

Next, we will have the qubit go through a Hadamard gate

$$H^{\otimes n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{k \cdot j} |j\rangle$$

($j \cdot k = j_0 k_0 \oplus j_1 k_1 \oplus \cdots \oplus j_{n-1} k_{n-1}$ is the sum of the bitwise product, where $\oplus$ is addition modulo 2) over the first register to obtain

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \right] = \sum_{y=0}^{2^n-1} \left[\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle$$

From this, we can see that the probability for a state k to be measured is

$$\left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot k} \right|^2$$

The probability of measuring $k = 0$, corresponding to $|0\rangle^{\otimes n}$, is

$$\left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2$$

which evaluates to 1 if $f(x)$ is constant (constructive interference) and 0 if $f(x)$ is balanced (destructive interference). In other words, the final measurement will be $|0\rangle^{\otimes n}$ (all zeros) if and only if $f(x)$ is constant and will yield some other state if $f(x)$ is balanced.

Deutsch's algorithm

Deutsch's algorithm is a special case of the general Deutsch–Jozsa algorithm where n = 1 in $f: \{0,1\}^n \to \{0,1\}$. We need to check the condition $f(0) = f(1)$. It is equivalent to check $f(0) \oplus f(1)$ (where $\oplus$ is addition modulo 2, which can also be viewed as a quantum XOR gate implemented as a Controlled NOT gate), if zero, then f is constant, otherwise f is not constant.

We begin with the two-qubit state $|0\rangle|1\rangle$ and apply a Hadamard gate to each qubit. This yields

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle).$$

We are given a quantum implementation of the function f that maps $|x\rangle|y\rangle$ to $|x\rangle|f(x) \oplus y\rangle$. Applying this function to our current state we obtain

$$\begin{aligned}
&\frac{1}{2}(|0\rangle(|f(0) \oplus 0\rangle - |f(0) \oplus 1\rangle) + |1\rangle(|f(1) \oplus 0\rangle - |f(1) \oplus 1\rangle)) \\
&= \frac{1}{2}((-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + (-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)) \\
&= (-1)^{f(0)}\frac{1}{2}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right)(|0\rangle - |1\rangle).
\end{aligned}$$

We ignore the last bit and the global phase and therefore have the state

$$\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle).$$

Applying a Hadamard gate to this state we have

$$\begin{aligned}
&\frac{1}{2}(|0\rangle + |1\rangle + (-1)^{f(0)\oplus f(1)}|0\rangle - (-1)^{f(0)\oplus f(1)}|1\rangle) \\
&= \frac{1}{2}((1 + (-1)^{f(0)\oplus f(1)})|0\rangle + (1 - (-1)^{f(0)\oplus f(1)})|1\rangle).
\end{aligned}$$

$f(0) \oplus f(1) = 0$ if and only if we measure $|0\rangle$ and $f(0) \oplus f(1) = 1$ if and only if we measure $|1\rangle$. So with certainty we know whether $f(x)$ is constant or balanced.

See also

- Bernstein–Vazirani algorithm

References

1. David Deutsch & Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". *Proceedings of the Royal Society of London A*. **439** (1907): 553–558. Bibcode:1992RSPSA.439..553D (https://ui.adsabs.harvard.edu/abs/1992RSPSA.439..553D). CiteSeerX 10.1.1.655.5997 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.655.5997). doi:10.1098/rspa.1992.0167 (https://doi.org/10.1098%2Frspa.1992.0167). S2CID 121702767 (https://api.semanticscholar.org/CorpusID:121702767).
2. R. Cleve; A. Ekert; C. Macchiavello; M. Mosca (1998). "Quantum algorithms revisited". *Proceedings of the Royal Society of London A*. **454** (1969): 339–354. arXiv:quant-ph/9708016 (https://arxiv.org/abs/quant-ph/9708016). Bibcode:1998RSPSA.454..339C (https://ui.adsabs.harvard.edu/abs/1998RSPSA.454..339C). doi:10.1098/rspa.1998.0164 (https://doi.org/10.1098%2Frspa.1998.0164). S2CID 16128238 (https://api.semanticscholar.org/CorpusID:16128238).
3. Simon, Daniel (November 1994). "On the power of quantum computation" (http://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.51.5477&rep=rep1&type=pdf). *Proceedings 35th Annual Symposium on Foundations of Computer Science*. pp. 116–123. doi:10.1109/SFCS.1994.365701 (https://doi.org/10.1109%2FSFCS.1994.365701). ISBN 0-8186-6580-7. S2CID 7457814 (https://api.semanticscholar.org/CorpusID:7457814).
4. Johansson, N.; Larsson, JÅ. (2017). "Efficient classical simulation of the Deutsch–Jozsa and Simon's algorithms". *Quantum Inf Process (2017)*. **16** (9): 233. arXiv:1508.05027 (https://arx

iv.org/abs/1508.05027). Bibcode:2017QuIP...16..233J (https://ui.adsabs.harvard.edu/abs/2017QuIP...16..233J). doi:10.1007/s11128-017-1679-7 (https://doi.org/10.1007%2Fs11128-017-1679-7). S2CID 28670540 (https://api.semanticscholar.org/CorpusID:28670540).

5. David Deutsch (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". *Proceedings of the Royal Society of London A*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D (https://ui.adsabs.harvard.edu/abs/1985RSPSA.400...97D). CiteSeerX 10.1.1.41.2382 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.2382). doi:10.1098/rspa.1985.0070 (https://doi.org/10.1098%2Frspa.1985.0070). S2CID 1438116 (https://api.semanticscholar.org/CorpusID:1438116).

External links

- Deutsch's lecture about the Deutsch-Jozsa algorithm (http://www.quiprocone.org/Protected/Lecture_5.htm)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Deutsch–Jozsa_algorithm&oldid=1236296482"

WIKIPEDIA
The Free Encyclopedia

Grover's algorithm

In quantum computing, **Grover's algorithm**, also known as the **quantum search algorithm**, is a quantum algorithm for unstructured search that finds with high probability the unique input to a black box function that produces a particular output value, using just $O(\sqrt{N})$ evaluations of the function, where N is the size of the function's domain. It was devised by Lov Grover in 1996.[1]

The analogous problem in classical computation cannot be solved in fewer than $O(N)$ evaluations (because, on average, one has to check half of the domain to get a 50% chance of finding the right input). Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani proved that any quantum solution to the problem needs to evaluate the function $\Omega(\sqrt{N})$ times, so Grover's algorithm is asymptotically optimal.[2] Since classical algorithms for NP-complete problems require exponentially many steps, and Grover's algorithm provides at most a quadratic speedup over the classical solution for unstructured search, this suggests that Grover's algorithm by itself will not provide polynomial-time solutions for NP-complete problems (as the square root of an exponential function is an exponential, not polynomial, function).[3]

Unlike other quantum algorithms, which may provide exponential speedup over their classical counterparts, Grover's algorithm provides only a quadratic speedup. However, even quadratic speedup is considerable when N is large, and Grover's algorithm can be applied to speed up broad classes of algorithms.[3] Grover's algorithm could brute-force a 128-bit symmetric cryptographic key in roughly 2^{64} iterations, or a 256-bit key in roughly 2^{128} iterations. It may not be the case that Grover's algorithm poses a significantly increased risk to encryption over existing classical algorithms, however.[4]

Applications and limitations

Grover's algorithm, along with variants like amplitude amplification, can be used to speed up a broad range of algorithms.[5][6][7] In particular, algorithms for NP-complete problems which contain exhaustive search as a subroutine can be sped up by Grover's algorithm.[6] The current theoretical best algorithm, in terms of worst-case complexity, for 3SAT is one such example. Generic constraint satisfaction problems also see quadratic speedups with Grover.[8] These algorithms do not require that the input be given in the form of an oracle, since Grover's algorithm is being applied with an explicit function, e.g. the function checking that a set of bits satisfies a 3SAT instance. However, it is unclear whether Grover's algorithm could speed up best practical algorithms for these problems.

Grover's algorithm can also give provable speedups for black-box problems in quantum query complexity, including element distinctness[9] and the collision problem[10] (solved with the Brassard–Høyer–Tapp algorithm). In these types of problems, one treats the oracle function *f* as a database, and the goal is to use the quantum query to this function as few times as possible.

Cryptography

Grover's algorithm essentially solves the task of *function inversion*. Roughly speaking, if we have a function $y = f(x)$ that can be evaluated on a quantum computer, Grover's algorithm allows us to calculate x when given y. Consequently, Grover's algorithm gives broad asymptotic speed-ups to many kinds of brute-force attacks on symmetric-key cryptography, including collision attacks and pre-image attacks.[11] However, this may not necessarily be the most efficient algorithm since, for example, the parallel rho algorithm is able to find a collision in SHA2 more efficiently than Grover's algorithm.[12]

Limitations

Grover's original paper described the algorithm as a database search algorithm, and this description is still common. The database in this analogy is a table of all of the function's outputs, indexed by the corresponding input. However, this database is not represented explicitly. Instead, an oracle is invoked to evaluate an item by its index. Reading a full database item by item and converting it into such a representation may take a lot longer than Grover's search. To account for such effects, Grover's algorithm can be viewed as solving an equation or satisfying a constraint. In such applications, the oracle is a way to check the constraint and is not related to the search algorithm. This separation usually prevents algorithmic optimizations, whereas conventional search algorithms often rely on such optimizations and avoid exhaustive search.[13] Fortunately, fast Grover's oracle implementation is possible for many constraint satisfaction and optimization problems.[14]

The major barrier to instantiating a speedup from Grover's algorithm is that the quadratic speedup achieved is too modest to overcome the large overhead of near-term quantum computers.[15] However, later generations of fault-tolerant quantum computers with better hardware performance may be able to realize these speedups for practical instances of data.

Problem description

As input for Grover's algorithm, suppose we have a function $f\colon \{0, 1, \dots, N-1\} \to \{0, 1\}$. In the "unstructured database" analogy, the domain represent indices to a database, and $f(x) = 1$ if and only if the data that x points to satisfies the search criterion. We additionally assume that only one index satisfies $f(x) = 1$, and we call this index ω. Our goal is to identify ω.

We can access f with a subroutine (sometimes called an oracle) in the form of a unitary operator U_ω that acts as follows:

$$\begin{cases} U_\omega|x\rangle = -|x\rangle & \text{for } x = \omega, \text{ that is, } f(x) = 1, \\ U_\omega|x\rangle = |x\rangle & \text{for } x \neq \omega, \text{ that is, } f(x) = 0. \end{cases}$$

This uses the N-dimensional state space $\mathcal{H}$, which is supplied by a register with $n = \lceil \log_2 N \rceil$ qubits. This is often written as

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle.$$

Grover's algorithm outputs ω with probability at least *1/2* using $O(\sqrt{N})$ applications of U_ω. This probability can be made arbitrarily large by running Grover's algorithm multiple times. If one runs Grover's algorithm until ω is found, the expected number of applications is still $O(\sqrt{N})$, since it will

only be run twice on average.

Alternative oracle definition

This section compares the above oracle U_ω with an oracle U_f.

U_ω is different from the standard quantum oracle for a function f. This standard oracle, denoted here as U_f, uses an ancillary qubit system. The operation then represents an inversion (NOT gate) on the main system conditioned by the value of $f(x)$ from the ancillary system:

$$\begin{cases} U_f|x\rangle|y\rangle = |x\rangle|\neg y\rangle & \text{for } x = \omega, \text{ that is, } f(x) = 1, \\ U_f|x\rangle|y\rangle = |x\rangle|y\rangle & \text{for } x \neq \omega, \text{ that is, } f(x) = 0, \end{cases}$$

or briefly,

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle.$$

These oracles are typically realized using uncomputation.

If we are given U_f as our oracle, then we can also implement U_ω, since U_ω is U_f when the ancillary qubit is in the state $|-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = H|1\rangle$:

$$\begin{aligned} U_f\big(|x\rangle \otimes |-\rangle\big) &= \frac{1}{\sqrt{2}}\left(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right) \\ &= \begin{cases} \frac{1}{\sqrt{2}}\left(-|x\rangle|0\rangle + |x\rangle|1\rangle\right) & \text{if } f(x) = 1, \\ \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) & \text{if } f(x) = 0 \end{cases} \\ &= (U_\omega|x\rangle) \otimes |-\rangle \end{aligned}$$

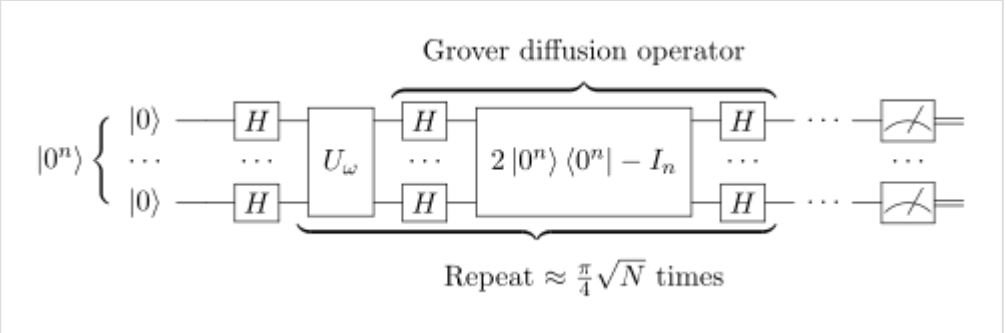
So, Grover's algorithm can be run regardless of which oracle is given.[3] If U_f is given, then we must maintain an additional qubit in the state $|-\rangle$ and apply U_f in place of U_ω.

Algorithm

The steps of Grover's algorithm are given as follows:

1. Initialize the system to the uniform superposition over all states $|s\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle.$
2. Perform the following "Grover iteration" $r(N)$ times:
    1. Apply the operator U_ω
    2. Apply the *Grover diffusion* operator $U_s = 2\,|s\rangle\,\langle s| - I$

3. Measure the resulting quantum state in the computational basis.



Quantum circuit representation of Grover's algorithm

For the correctly chosen value of r, the output will be $|\omega\rangle$ with probability approaching 1 for $N \gg 1$. Analysis shows that this eventual value for $r(N)$ satisfies $r(N) \leq \left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

Implementing the steps for this algorithm can be done using a number of gates linear in the number of qubits.[3] Thus, the gate complexity of this algorithm is $O(\log(N)r(N))$, or $O(\log(N))$ per iteration.

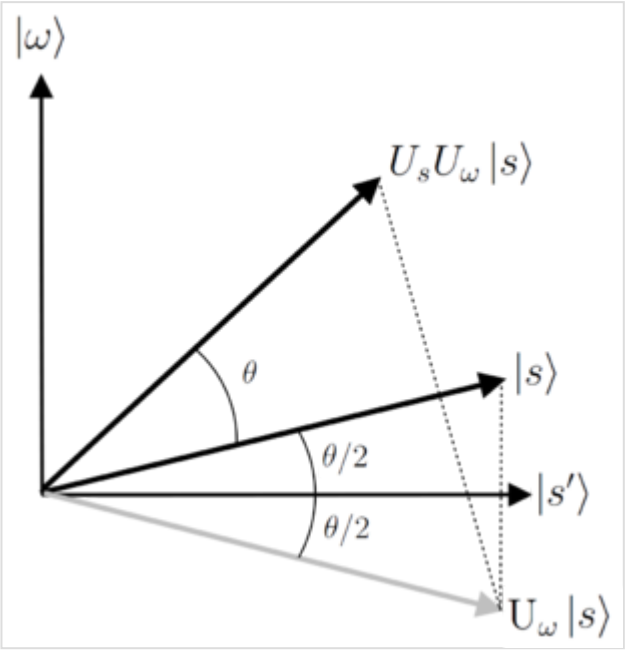
Geometric proof of correctness

There is a geometric interpretation of Grover's algorithm, following from the observation that the quantum state of Grover's algorithm stays in a two-dimensional subspace after each step. Consider the plane spanned by $|s\rangle$ and $|\omega\rangle$; equivalently, the plane spanned by $|\omega\rangle$ and the perpendicular ket $|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$.

Grover's algorithm begins with the initial ket $|s\rangle$, which lies in the subspace. The operator U_ω is a reflection at the hyperplane orthogonal to $|\omega\rangle$ for vectors in the plane spanned by $|s'\rangle$ and $|\omega\rangle$, i.e. it acts as a reflection across $|s'\rangle$. This can be seen by writing U_ω in the form of a Householder reflection:

$$U_\omega = I - 2|\omega\rangle\langle\omega|.$$

The operator $U_s = 2|s\rangle\langle s| - I$ is a reflection through $|s\rangle$. Both operators U_s and U_ω take states in the plane spanned by $|s'\rangle$ and $|\omega\rangle$ to states in the plane. Therefore, Grover's algorithm stays in this plane for the entire algorithm.



Picture showing the geometric interpretation of the first iteration of Grover's algorithm. The state vector $|s\rangle$ is rotated towards the target vector $|\omega\rangle$ as shown.

It is straightforward to check that the operator $U_s U_\omega$ of each Grover iteration step rotates the state vector by an angle of $\theta = 2 \arcsin \frac{1}{\sqrt{N}}$. So, with enough iterations, one can rotate from the initial state $|s\rangle$ to the desired output state $|\omega\rangle$. The initial ket is close to the state orthogonal to $|\omega\rangle$:

$$\langle s' | s \rangle = \sqrt{\frac{N-1}{N}}.$$

In geometric terms, the angle $\theta/2$ between $|s\rangle$ and $|s'\rangle$ is given by

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}}.$$

We need to stop when the state vector passes close to $|\omega\rangle$; after this, subsequent iterations rotate the state vector *away* from $|\omega\rangle$, reducing the probability of obtaining the correct answer. The exact probability of measuring the correct answer is

$$\sin^2\left(\left(r+\frac{1}{2}\right)\theta\right),$$

where *r* is the (integer) number of Grover iterations. The earliest time that we get a near-optimal measurement is therefore $r \approx \pi\sqrt{N}/4$.

Algebraic proof of correctness

To complete the algebraic analysis, we need to find out what happens when we repeatedly apply $U_s U_\omega$. A natural way to do this is by eigenvalue analysis of a matrix. Notice that during the entire computation, the state of the algorithm is a linear combination of s and ω. We can write the action of U_s and U_ω in the space spanned by $\{|s\rangle, |\omega\rangle\}$ as:

$$U_s : a|\omega\rangle + b|s\rangle \mapsto [|\omega\rangle\ |s\rangle] \begin{bmatrix} -1 & 0 \\ 2/\sqrt{N} & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}.$$

$$U_\omega : a|\omega\rangle + b|s\rangle \mapsto [|\omega\rangle\ |s\rangle] \begin{bmatrix} -1 & -2/\sqrt{N} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}.$$

So in the basis $\{|\omega\rangle, |s\rangle\}$ (which is neither orthogonal nor a basis of the whole space) the action $U_s U_\omega$ of applying U_ω followed by U_s is given by the matrix

$$U_s U_\omega = \begin{bmatrix} -1 & 0 \\ 2/\sqrt{N} & 1 \end{bmatrix} \begin{bmatrix} -1 & -2/\sqrt{N} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2/\sqrt{N} \\ -2/\sqrt{N} & 1-4/N \end{bmatrix}.$$

This matrix happens to have a very convenient Jordan form. If we define $t = \arcsin(1/\sqrt{N})$, it is

$$U_s U_\omega = M \begin{bmatrix} e^{2it} & 0 \\ 0 & e^{-2it} \end{bmatrix} M^{-1} \text{ where } M = \begin{bmatrix} -i & i \\ e^{it} & e^{-it} \end{bmatrix}.$$

It follows that *r*-th power of the matrix (corresponding to *r* iterations) is

$$(U_s U_\omega)^r = M \begin{bmatrix} e^{2rit} & 0 \\ 0 & e^{-2rit} \end{bmatrix} M^{-1}.$$

Using this form, we can use trigonometric identities to compute the probability of observing ω after r iterations mentioned in the previous section,

$$\left| \begin{bmatrix} \langle \omega | \omega \rangle & \langle \omega | s \rangle \end{bmatrix} (U_s U_\omega)^r \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right|^2 = \sin^2((2r+1)t).$$

Alternatively, one might reasonably imagine that a near-optimal time to distinguish would be when the angles $2rt$ and $-2rt$ are as far apart as possible, which corresponds to $2rt \approx \pi/2$, or $r = \pi/4t = \pi/4 \arcsin(1/\sqrt{N}) \approx \pi\sqrt{N}/4$. Then the system is in state

$$\begin{bmatrix} |\omega\rangle & |s\rangle \end{bmatrix} (U_s U_\omega)^r \begin{bmatrix} 0 \\ 1 \end{bmatrix} \approx \begin{bmatrix} |\omega\rangle & |s\rangle \end{bmatrix} M \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} M^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |\omega\rangle \frac{1}{\cos(t)} - |s\rangle \frac{\sin(t)}{\cos(t)}.$$

A short calculation now shows that the observation yields the correct answer ω with error $O\left(\frac{1}{N}\right)$.

Extensions and variants

Multiple matching entries

If, instead of 1 matching entry, there are k matching entries, the same algorithm works, but the number of iterations must be $\frac{\pi}{4}\left(\frac{N}{k}\right)^{1/2}$ instead of $\frac{\pi}{4}N^{1/2}$.

There are several ways to handle the case if k is unknown.[16] A simple solution performs optimally up to a constant factor: run Grover's algorithm repeatedly for increasingly small values of k, e.g., taking $k = N$, $N/2$, $N/4$, ..., and so on, taking $k = N/2^t$ for iteration t until a matching entry is found.

With sufficiently high probability, a marked entry will be found by iteration $t = \log_2(N/k) + c$ for some constant c. Thus, the total number of iterations taken is at most

$$\frac{\pi}{4}\left(1 + \sqrt{2} + \sqrt{4} + \cdots + \sqrt{\frac{N}{k2^c}}\right) = O(\sqrt{N/k}).$$

Another approach if k is unknown is to derive it via the quantum counting algorithm prior.

If $k = N/2$ (or the traditional one marked state Grover's Algorithm if run with $N = 2$), the algorithm will provide no amplification. If $k > N/2$, increasing k will begin to increase the number of iterations necessary to obtain a solution.[17] On the other hand, if $k \geq N/2$, a classical running of the checking oracle on a single random choice of input will more likely than not give a correct solution.

A version of this algorithm is used in order to solve the collision problem.[18][19]

Quantum partial search

A modification of Grover's algorithm called quantum partial search was described by Grover and Radhakrishnan in 2004.[20] In partial search, one is not interested in finding the exact address of the target item, only the first few digits of the address. Equivalently, we can think of "chunking" the search space into blocks, and then asking "in which block is the target item?". In many applications, such a search yields enough information if the target address contains the information wanted. For instance, to use the example given by L. K. Grover, if one has a list of students organized by class rank, we may only be interested in whether a student is in the lower 25%, 25–50%, 50–75% or 75–100% percentile.

To describe partial search, we consider a database separated into K blocks, each of size $b = N/K$. The partial search problem is easier. Consider the approach we would take classically – we pick one block at random, and then perform a normal search through the rest of the blocks (in set theory language, the complement). If we don't find the target, then we know it's in the block we didn't search. The average number of iterations drops from $N/2$ to $(N - b)/2$.

Grover's algorithm requires $\frac{\pi}{4}\sqrt{N}$ iterations. Partial search will be faster by a numerical factor that depends on the number of blocks K. Partial search uses n_1 global iterations and n_2 local iterations. The global Grover operator is designated G_1 and the local Grover operator is designated G_2.

The global Grover operator acts on the blocks. Essentially, it is given as follows:

1. Perform j_1 standard Grover iterations on the entire database.
2. Perform j_2 local Grover iterations. A local Grover iteration is a direct sum of Grover iterations over each block.
3. Perform one standard Grover iteration.

The optimal values of j_1 and j_2 are discussed in the paper by Grover and Radhakrishnan. One might also wonder what happens if one applies successive partial searches at different levels of "resolution". This idea was studied in detail by Vladimir Korepin and Xu, who called it binary quantum search. They proved that it is not in fact any faster than performing a single partial search.

Optimality

Grover's algorithm is optimal up to sub-constant factors. That is, any algorithm that accesses the database only by using the operator U_ω must apply U_ω at least a $1 - o(1)$ fraction as many times as Grover's algorithm.[21] The extension of Grover's algorithm to k matching entries, $\pi(N/k)^{1/2}/4$, is also optimal.[18] This result is important in understanding the limits of quantum computation.

If the Grover's search problem was solvable with $\log^c N$ applications of U_ω, that would imply that NP is contained in BQP, by transforming problems in NP into Grover-type search problems. The optimality of Grover's algorithm suggests that quantum computers cannot solve NP-Complete problems in polynomial time, and thus NP is not contained in BQP.

It has been shown that a class of non-local hidden variable quantum computers could implement a search of an N-item database in at most $O(\sqrt[3]{N})$ steps. This is faster than the $O(\sqrt{N})$ steps taken by Grover's algorithm.[22]

See also

- Amplitude amplification
- Brassard–Høyer–Tapp algorithm (for solving the collision problem)
- Shor's algorithm (for factorization)
- Quantum walk search

Notes

1. Grover, Lov K. (1996-07-01). "A fast quantum mechanical algorithm for database search" (https://doi.org/10.1145/237814.237866). *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. Philadelphia, Pennsylvania, USA: Association for Computing Machinery. pp. 212–219. arXiv:quant-ph/9605043 (https://arxiv.org/abs/quant-ph/9605043). Bibcode:1996quant.ph..5043G (https://ui.adsabs.harvard.edu/abs/1996quant.ph..5043G). doi:10.1145/237814.237866 (https://doi.org/10.1145%2F237814.237866). ISBN 978-0-89791-785-8. S2CID 207198067 (https://api.semanticscholar.org/CorpusID:207198067).
2. Bennett C.H.; Bernstein E.; Brassard G.; Vazirani U. (1997). "The strengths and weaknesses of quantum computation" (http://www.cs.berkeley.edu/~vazirani/pubs/bbbv.ps). *SIAM Journal on Computing*. **26** (5): 1510–1523. arXiv:quant-ph/9701001 (https://arxiv.org/abs/quant-ph/9701001). doi:10.1137/s0097539796300933 (https://doi.org/10.1137%2Fs0097539796300933). S2CID 13403194 (https://api.semanticscholar.org/CorpusID:13403194).
3. Nielsen, Michael A. (2010). *Quantum computation and quantum information* (https://www.worldcat.org/oclc/665137861). Isaac L. Chuang. Cambridge: Cambridge University Press. pp. 276–305. ISBN 978-1-107-00217-3. OCLC 665137861 (https://search.worldcat.org/oclc/665137861).
4. Bernstein, Daniel J. (2010). "Grover vs. McEliece" (https://cr.yp.to/codes/grovercode-20100303.pdf) (PDF). In Sendrier, Nicolas (ed.). *Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings*. Lecture Notes in Computer Science. Vol. 6061. Springer. pp. 73–80. doi:10.1007/978-3-642-12929-2_6 (https://doi.org/10.1007%2F978-3-642-12929-2_6).
5. Grover, Lov K. (1998). "A framework for fast quantum mechanical algorithms". In Vitter, Jeffrey Scott (ed.). *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23–26, 1998*. Association for Computing Machinery. pp. 53–62. arXiv:quant-ph/9711043 (https://arxiv.org/abs/quant-ph/9711043). doi:10.1145/276698.276712 (https://doi.org/10.1145%2F276698.276712).
6. Ambainis, A. (2004-06-01). "Quantum search algorithms" (https://doi.org/10.1145/992287.992296). *ACM SIGACT News*. **35** (2): 22–35. arXiv:quant-ph/0504012 (https://arxiv.org/abs/quant-ph/0504012). doi:10.1145/992287.992296 (https://doi.org/10.1145%2F992287.992296). ISSN 0163-5700 (https://search.worldcat.org/issn/0163-5700). S2CID 11326499 (https://api.semanticscholar.org/CorpusID:11326499).
7. Jordan, Stephen. "Quantum Algorithm Zoo" (https://quantumalgorithmzoo.org). *quantumalgorithmzoo.org*. Retrieved 2021-04-21.

8. Cerf, Nicolas J.; Grover, Lov K.; Williams, Colin P. (2000-05-01). "Nested Quantum Search and NP-Hard Problems" (https://doi.org/10.1007/s002000050134). *Applicable Algebra in Engineering, Communication and Computing*. **10** (4): 311–338. doi:10.1007/s002000050134 (https://doi.org/10.1007%2Fs002000050134). ISSN 1432-0622 (https://search.worldcat.org/issn/1432-0622). S2CID 311132 (https://api.semanticscholar.org/CorpusID:311132).
9. Ambainis, Andris (2007-01-01). "Quantum Walk Algorithm for Element Distinctness" (https://epubs.siam.org/doi/10.1137/S0097539705447311). *SIAM Journal on Computing*. **37** (1): 210–239. arXiv:quant-ph/0311001 (https://arxiv.org/abs/quant-ph/0311001). doi:10.1137/S0097539705447311 (https://doi.org/10.1137%2FS0097539705447311). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397). S2CID 6581885 (https://api.semanticscholar.org/CorpusID:6581885).
10. Brassard, Gilles; Høyer, Peter; Tapp, Alain (1998). "Quantum Cryptanalysis of Hash and Claw-Free Functions". In Lucchesi, Claudio L.; Moura, Arnaldo V. (eds.). *LATIN '98: Theoretical Informatics, Third Latin American Symposium, Campinas, Brazil, April, 20-24, 1998, Proceedings*. Lecture Notes in Computer Science. Vol. 1380. Springer. pp. 163–169. arXiv:quant-ph/9705002 (https://arxiv.org/abs/quant-ph/9705002). doi:10.1007/BFb0054319 (https://doi.org/10.1007%2FBFb0054319).
11. *Post-quantum cryptography* (https://www.worldcat.org/oclc/318545517). Daniel J. Bernstein, Johannes Buchmann, Erik, Dipl.-Math Dahmén. Berlin: Springer. 2009. ISBN 978-3-540-88702-7. OCLC 318545517 (https://search.worldcat.org/oclc/318545517).
12. Bernstein, Daniel J. (2021-04-21). "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?" (https://www.hyperelliptic.org/tanja/SHARCS/record2.pdf#page=113) (PDF). *Conference Proceedings for Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS '09)*. **09**: 105–117.
13. Viamontes G.F.; Markov I.L.; Hayes J.P. (2005), "Is Quantum Search Practical?" (https://web.eecs.umich.edu/~imarkov/pubs/jour/cise05-grov.pdf) (PDF), *Computing in Science and Engineering*, **7** (3): 62–70, arXiv:quant-ph/0405001 (https://arxiv.org/abs/quant-ph/0405001), Bibcode:2005CSE.....7c..62V (https://ui.adsabs.harvard.edu/abs/2005CSE.....7c..62V), doi:10.1109/mcse.2005.53 (https://doi.org/10.1109%2Fmcse.2005.53), S2CID 8929938 (https://api.semanticscholar.org/CorpusID:8929938)
14. Sinitsyn N. A.; Yan B. (2023). "Topologically protected Grover's oracle for the partition problem". *Physical Review A*. **108** (2): 022412. arXiv:2304.10488 (https://arxiv.org/abs/2304.10488). doi:10.1103/PhysRevA.108.022412 (https://doi.org/10.1103%2FPhysRevA.108.022412). S2CID 258236417 (https://api.semanticscholar.org/CorpusID:258236417).
15. Babbush, Ryan; McClean, Jarrod R.; Newman, Michael; Gidney, Craig; Boixo, Sergio; Neven, Hartmut (2021-03-29). "Focus beyond Quadratic Speedups for Error-Corrected Quantum Advantage" (https://doi.org/10.1103%2FPRXQuantum.2.010103). *PRX Quantum*. **2** (1): 010103. arXiv:2011.04149 (https://arxiv.org/abs/2011.04149). doi:10.1103/PRXQuantum.2.010103 (https://doi.org/10.1103%2FPRXQuantum.2.010103).
16. Aaronson, Scott (April 19, 2021). "Introduction to Quantum Information Science Lecture Notes" (https://www.scottaaronson.com/qclec.pdf) (PDF).
17. Nielsen-Chuang
18. Michel Boyer; Gilles Brassard; Peter Høyer; Alain Tapp (1998), "Tight Bounds on Quantum Searching", *Fortschr. Phys.*, **46** (4–5): 493–506, arXiv:quant-ph/9605034 (https://arxiv.org/abs/quant-ph/9605034), Bibcode:1998ForPh..46..493B (https://ui.adsabs.harvard.edu/abs/1998ForPh..46..493B), doi:10.1002/3527603093.ch10 (https://doi.org/10.1002%2F3527603093.ch10), ISBN 9783527603091
19. Andris Ambainis (2004), "Quantum search algorithms", *SIGACT News*, **35** (2): 22–35, arXiv:quant-ph/0504012 (https://arxiv.org/abs/quant-ph/0504012), Bibcode:2005quant.ph..4012A (https://ui.adsabs.harvard.edu/abs/2005quant.ph..4012A), doi:10.1145/992287.992296 (https://doi.org/10.1145%2F992287.992296), S2CID 11326499 (https://api.semanticscholar.org/CorpusID:11326499)

20. L.K. Grover; J. Radhakrishnan (2005-02-07). "Is partial quantum search of a database any easier?". arXiv:quant-ph/0407122v4 (https://arxiv.org/abs/quant-ph/0407122v4).
21. Zalka, Christof (1999-10-01). "Grover's quantum searching algorithm is optimal" (https://link.aps.org/doi/10.1103/PhysRevA.60.2746). *Physical Review A*. **60** (4): 2746–2751. arXiv:quant-ph/9711070 (https://arxiv.org/abs/quant-ph/9711070). Bibcode:1999PhRvA..60.2746Z (https://ui.adsabs.harvard.edu/abs/1999PhRvA..60.2746Z). doi:10.1103/PhysRevA.60.2746 (https://doi.org/10.1103%2FPhysRevA.60.2746). S2CID 1542077 (https://api.semanticscholar.org/CorpusID:1542077).
22. Aaronson, Scott. "Quantum Computing and Hidden Variables" (http://www.scottaaronson.com/papers/qchvpra.pdf) (PDF).

References

- Grover L.K.: *A fast quantum mechanical algorithm for database search (https://arxiv.org/abs/quant-ph/9605043)*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212
- Grover L.K.: *From Schrödinger's equation to quantum search algorithm (https://arxiv.org/abs/quant-ph/0109116)*, American Journal of Physics, 69(7): 769–777, 2001. Pedagogical review of the algorithm and its history.
- Grover L.K.: QUANTUM COMPUTING: How the weird logic of the subatomic world could make it possible for machines to calculate millions of times faster than they do today (https://cryptome.org/qc-grover.htm) *The Sciences*, July/August 1999, pp. 24–30.
- Nielsen, M.A. and Chuang, I.L. *Quantum computation and quantum information*. Cambridge University Press, 2000. Chapter 6.
- What's a Quantum Phone Book? (https://web.archive.org/web/20140201230754/http://www.bell-labs.com/user/feature/archives/lkgrover/), Lov Grover, Lucent Technologies

External links

- Davy Wybiral. "Quantum Circuit Simulator" (https://web.archive.org/web/20170116155032/http://davy.wtf/quantum/?example=Grover%27s%20Algorithm). Archived from the original (http://davy.wtf/quantum/?example=Grover%27s%20Algorithm) on 2017-01-16. Retrieved 2017-01-13.
- Craig Gidney (2013-03-05). "Grover's Quantum Search Algorithm" (https://web.archive.org/web/20201117095032/http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm). Archived from the original (http://twistedoakstudios.com/blog/Post2644_grovers-quantum-search-algorithm) on 2020-11-17. Retrieved 2013-03-08.
- François Schwarzentruber (2013-05-18). "Grover's algorithm" (http://people.irisa.fr/Francois.Schwarzentruber/mit1_algo2_2013/grover_s_algorithm/).
- Alexander Prokopenya. "Quantum Circuit Implementing Grover's Search Algorithm" (http://demonstrations.wolfram.com/QuantumCircuitImplementingGroversSearchAlgorithm/). Wolfram Alpha.
- "Quantum computation, theory of" (https://www.encyclopediaofmath.org/index.php?title=Quantum_computation,_theory_of), *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]
- Roberto Maestre (2018-05-11). "Grover's Algorithm implemented in R and C" (https://github.com/rmaestre/quantumSystem). *GitHub*.
- Bernhard Ömer. "QCL - A Programming Language for Quantum Computers" (http://tph.tuwien.ac.at/~oemer/qcl.html). Retrieved 2022-04-30. "Implemented in /qcl-0.6.4/lib/grover.qcl"

Retrieved from "https://en.wikipedia.org/w/index.php?title=Grover%27s_algorithm&oldid=1239261162"

WIKIPEDIA
The Free Encyclopedia

HHL algorithm

The **Harrow–Hassidim–Lloyd algorithm** or **HHL algorithm** is a quantum algorithm for numerically solving a system of linear equations, designed by Aram Harrow, Avinatan Hassidim, and Seth Lloyd. The algorithm estimates the result of a scalar measurement on the solution vector to a given linear system of equations.[1]

The algorithm is one of the main fundamental algorithms expected to provide a speedup over their classical counterparts, along with Shor's factoring algorithm, Grover's search algorithm, and the quantum Fourier transform. Provided the linear system is sparse[2] and has a low condition number κ, and that the user is interested in the result of a scalar measurement on the solution vector, instead of the values of the solution vector itself, then the algorithm has a runtime of $O(\log(N)\kappa^2)$, where N is the number of variables in the linear system. This offers an exponential speedup over the fastest classical algorithm, which runs in $O(N\kappa)$ (or $O(N\sqrt{\kappa})$ for positive semidefinite matrices).

An implementation of the quantum algorithm for linear systems of equations was first demonstrated in 2013 by three independent publications.[3][4][5] The demonstrations consisted of simple linear equations on specially designed quantum devices.[3][4][5] The first demonstration of a general-purpose version of the algorithm appeared in 2018.[6]

Due to the prevalence of linear systems in virtually all areas of science and engineering, the quantum algorithm for linear systems of equations has the potential for widespread applicability.[7]

Procedure

The HHL algorithm tackles the following problem: given a $N \times N$ Hermitian matrix A and a unit vector $\vec{b} \in \mathbb{R}^N$, prepare the quantum state $|x\rangle$ corresponding to the vector $\vec{x} \in \mathbb{R}^N$ that solves the linear system $A\vec{x} = \vec{b}$. More precisely, the goal is to prepare a state $|x\rangle$ whose amplitudes equal the elements of $\vec{x}$. This means, in particular, that the algorithm cannot be used to efficiently retrieve the vector $\vec{x}$ itself. It does, however, allow to efficiently compute expectation values of the form $\langle x|M|x\rangle$ for some observable M.

First, the algorithm represents the vector $\vec{b}$ as a quantum state of the form:

$$|b\rangle = \sum_{i=1}^{N} b_i |i\rangle.$$

Next, Hamiltonian simulation techniques are used to apply the unitary operator e^{iAt} to $|b\rangle$ for a superposition of different times t. The ability to decompose $|b\rangle$ into the eigenbasis of A and to find the corresponding eigenvalues λ_j is facilitated by the use of quantum phase estimation.

The state of the system after this decomposition is approximately:

$$\sum_{j=1}^{N} \beta_j |u_j\rangle |\lambda_j\rangle,$$

where u_j is the eigenvector basis of A, and $|b\rangle = \sum_{j=1}^{N} \beta_j |u_j\rangle$.

We would then like to perform the linear map taking $|\lambda_j\rangle$ to $C\lambda_j^{-1}|\lambda_j\rangle$, where C is a normalizing constant. The linear mapping operation is not unitary and thus will require a number of repetitions as it has some probability of failing. After it succeeds, we uncomputed the $|\lambda_j\rangle$ register and are left with a state proportional to:

$$\sum_{i=1}^{N} \beta_i \lambda_j^{-1} |u_j\rangle = A^{-1}|b\rangle = |x\rangle,$$

where $|x\rangle$ is a quantum-mechanical representation of the desired solution vector *x*. To read out all components of *x* would require the procedure be repeated at least *N* times. However, it is often the case that one is not interested in x itself, but rather some expectation value of a linear operator *M* acting on *x*. By mapping *M* to a quantum-mechanical operator and performing the quantum measurement corresponding to *M*, we obtain an estimate of the expectation value $\langle x|M|x\rangle$. This allows for a wide variety of features of the vector *x* to be extracted including normalization, weights in different parts of the state space, and moments without actually computing all the values of the solution vector *x*.

Explanation

Initialization

Firstly, the algorithm requires that the matrix A be Hermitian so that it can be converted into a unitary operator. In the case where A is not Hermitian, define

$$\mathbf{C} = \begin{bmatrix} 0 & A \\ A^\dagger & 0 \end{bmatrix}.$$

As C is Hermitian, the algorithm can now be used to solve $Cy = \begin{bmatrix} b \\ 0 \end{bmatrix}$ to obtain $y = \begin{bmatrix} 0 \\ x \end{bmatrix}$.

Secondly, the algorithm requires an efficient procedure to prepare $|b\rangle$, the quantum representation of b. It is assumed that there exists some linear operator B that can take some arbitrary quantum state $|\mathbf{initial}\rangle$ to $|b\rangle$ efficiently or that this algorithm is a subroutine in a larger algorithm and is given $|b\rangle$ as input. Any error in the preparation of state $|b\rangle$ is ignored.

Finally, the algorithm assumes that the state $|\psi_0\rangle$ can be prepared efficiently, where

$$|\psi_0\rangle := \sqrt{2/T} \sum_{\tau=0}^{T-1} \sin \pi \left(\frac{\tau + \frac{1}{2}}{T} \right) |\tau\rangle$$

for some large T. The coefficients of $|\psi_0\rangle$ are chosen to minimize a certain quadratic loss function which induces error in the U_{invert} subroutine described below.

Hamiltonian simulation

Hamiltonian simulation is used to transform the Hermitian matrix A into a unitary operator, which can then be applied at will. This is possible if A is s-sparse and efficiently row computable, meaning it has at most s nonzero entries per row and given a row index these entries can be computed in time O(s). Under these assumptions, quantum Hamiltonian simulation allows e^{iAt} to be simulated in time $O(\log(N)s^2t)$.

U_{invert} subroutine

The key subroutine to the algorithm, denoted U_{invert}, is defined as follows and incorporates a phase estimation subroutine:

1. Prepare $|\psi_0\rangle^C$ on register C

2. Apply the conditional Hamiltonian evolution (sum)

3. Apply the Fourier transform to the register C. Denote the resulting basis states with $|k\rangle$ for $k = 0, ..., T - 1$. Define $\lambda_k := 2\pi k/t_0$.

4. Adjoin a three-dimensional register S in the state

$$|h(\lambda_k)\rangle^S := \sqrt{1 - f(\lambda_k)^2 - g(\lambda_k)^2}|\text{nothing}\rangle^S + f(\lambda_k)|\text{well}\rangle^S + g(\lambda_k)|\text{ill}\rangle^S,$$

5. Reverse steps 1–3, uncomputing any garbage produced along the way.

The phase estimation procedure in steps 1-3 allows for the estimation of eigenvalues of A up to error ϵ.

The ancilla register in step 4 is necessary to construct a final state with inverted eigenvalues corresponding to the diagonalized inverse of A. In this register, the functions f, g, are called filter functions. The states 'nothing', 'well' and 'ill' are used to instruct the loop body on how to proceed; 'nothing' indicates that the desired matrix inversion has not yet taken place, 'well' indicates that the inversion has taken place and the loop should halt, and 'ill' indicates that part of $|b\rangle$ is in the ill-conditioned subspace of A and the algorithm will not be able to produce the desired inversion. Producing a state proportional to the inverse of A requires 'well' to be measured, after which the overall state of the system collapses to the desired state by the extended Born rule.

Main loop

The body of the algorithm follows the amplitude amplification procedure: starting with $U_{\text{invert}}B|\text{initial}\rangle$, the following operation is repeatedly applied:

$$U_{\text{invert}}BR_{\text{init}}B^\dagger U_{\text{invert}}^\dagger R_{\text{succ}},$$

where

$$R_{\text{succ}} = I - 2|\text{well}\rangle\langle\text{well}|$$

and

$$R_{\text{init}} = I - 2|\text{initial}\rangle\langle\text{initial}|.$$

After each repetition, S is measured and will produce a value of 'nothing', 'well', or 'ill' as described above. This loop is repeated until $|\text{well}\rangle$ is measured, which occurs with a probability p. Rather than repeating $\frac{1}{p}$ times to minimize error, amplitude amplification is used to achieve the same error resilience using only $O\left(\frac{1}{\sqrt{p}}\right)$ repetitions.

Scalar measurement

After successfully measuring 'well' on S the system will be in a state proportional to:

$$\sum_{i=1}^{N} \beta_i \lambda_j^{-1} |u_j\rangle = A^{-1}|b\rangle = |x\rangle.$$

Finally, we perform the quantum-mechanical operator corresponding to M and obtain an estimate of the value of $\langle x|M|x\rangle$.

Run time analysis

Classical efficiency

The best classical algorithm which produces the actual solution vector $\vec{x}$ is Gaussian elimination, which runs in $O(N^3)$ time.

If *A* is *s*-sparse and positive semi-definite, then the Conjugate Gradient method can be used to find the solution vector $\vec{x}$, which can be found in $O(Ns\kappa)$ time by minimizing the quadratic function $|A\vec{x} - \vec{b}|^2$.

When only a summary statistic of the solution vector $\vec{x}$ is needed, as is the case for the quantum algorithm for linear systems of equations, a classical computer can find an estimate of $\vec{x}^\dagger M\vec{x}$ in $O(N\sqrt{\kappa})$.

Quantum efficiency

The runtime of the quantum algorithm for solving systems of linear equations originally proposed by Harrow et al. was shown to be $O(\kappa^2 \log N/\varepsilon)$, where $\varepsilon > 0$ is the error parameter and κ is the condition number of A. This was subsequently improved to $O(\kappa \log^3 \kappa \log N/\varepsilon^3)$ by Andris Ambainis[8] and a quantum algorithm with runtime polynomial in $\log(1/\varepsilon)$ was developed by Childs et al.[9] Since the HHL algorithm maintains its logarithmic scaling in N only for sparse or low rank matrices, Wossnig et

al.[10] extended the HHL algorithm based on a quantum singular value estimation technique and provided a linear system algorithm for dense matrices which runs in $O(\sqrt{N}\log N\kappa^2)$ time compared to the $O(N\log N\kappa^2)$ of the standard HHL algorithm.

Optimality

An important factor in the performance of the matrix inversion algorithm is the condition number κ, which represents the ratio of A's largest and smallest eigenvalues. As the condition number increases, the ease with which the solution vector can be found using gradient descent methods such as the conjugate gradient method decreases, as A becomes closer to a matrix which cannot be inverted and the solution vector becomes less stable. This algorithm assumes that all singular values of the matrix A lie between $\frac{1}{\kappa}$ and 1, in which case the claimed run-time proportional to κ^2 will be achieved. Therefore, the speedup over classical algorithms is increased further when κ is a $\mathrm{poly}(\log(N))$.[1]

If the run-time of the algorithm were made poly-logarithmic in κ then problems solvable on *n* qubits could be solved in poly(*n*) time, causing the complexity class BQP to be equal to PSPACE.[1]

Error analysis

Performing the Hamiltonian simulation, which is the dominant source of error, is done by simulating e^{iAt}. Assuming that A is s-sparse, this can be done with an error bounded by a constant ε, which will translate to the additive error achieved in the output state $|x\rangle$.

The phase estimation step errs by $O\left(\frac{1}{t_0}\right)$ in estimating λ, which translates into a relative error of $O\left(\frac{1}{\lambda t_0}\right)$ in λ^{-1}. If $\lambda \geq 1/\kappa$, taking $t_0 = O(\kappa\varepsilon)$ induces a final error of ε. This requires that the overall run-time efficiency be increased proportional to $O\left(\frac{1}{\varepsilon}\right)$ to minimize error.

Experimental realization

While there does not yet exist a quantum computer that can truly offer a speedup over a classical computer, implementation of a "proof of concept" remains an important milestone in the development of a new quantum algorithm. Demonstrating the quantum algorithm for linear systems of equations remained a challenge for years after its proposal until 2013 when it was demonstrated by Cai et al., Barz et al. and Pan et al. in parallel.

Cai et al.

Published in Physical Review Letters 110, 230501 (2013), Cai et al. reported an experimental demonstration of the simplest meaningful instance of this algorithm, that is, solving 2×2 linear equations for various input vectors. The quantum circuit is optimized and compiled into a linear optical network with four photonic quantum bits (qubits) and four controlled logic gates, which is used to

coherently implement every subroutine for this algorithm. For various input vectors, the quantum computer gives solutions for the linear equations with reasonably high precision, ranging from fidelities of 0.825 to 0.993.[11]

Barz et al.

On February 5, 2013, Stefanie Barz and co-workers demonstrated the quantum algorithm for linear systems of equations on a photonic quantum computing architecture. This implementation used two consecutive entangling gates on the same pair of polarization-encoded qubits. Two separately controlled NOT gates were realized where the successful operation of the first was heralded by a measurement of two ancillary photons. Barz et al. found that the fidelity in the obtained output state ranged from 64.7% to 98.1% due to the influence of higher-order emissions from spontaneous parametric down-conversion.[4]

Pan et al.

On February 8, 2013, Pan et al. reported a proof-of-concept experimental demonstration of the quantum algorithm using a 4-qubit nuclear magnetic resonance quantum information processor. The implementation was tested using simple linear systems of only 2 variables. Across three experiments they obtain the solution vector with over 96% fidelity.[5]

Wen et al.

Another experimental demonstration using NMR for solving an 8*8 system was reported by Wen et al.[12] in 2018 using the algorithm developed by Subaşı et al.[13]

Applications

Quantum computers are devices that harness quantum mechanics to perform computations in ways that classical computers cannot. For certain problems, quantum algorithms supply exponential speedups over their classical counterparts, the most famous example being Shor's factoring algorithm. Few such exponential speedups are known, and those that are (such as the use of quantum computers to simulate other quantum systems) have so far found limited practical use due to the current small size of quantum computers. This algorithm provides an exponentially faster method of estimating features of the solution of a set of linear equations, which is a problem ubiquitous in science and engineering, both on its own and as a subroutine in more complex problems.

Electromagnetic scattering

Clader et al. provided a preconditioned version of the linear systems algorithm that provided two advances. First, they demonstrated how a preconditioner could be included within the quantum algorithm. This expands the class of problems that can achieve the promised exponential speedup, since the scaling of HHL and the best classical algorithms are both polynomial in the condition number. The second

advance was the demonstration of how to use HHL to solve for the radar cross-section of a complex shape. This was one of the first end to end examples of how to use HHL to solve a concrete problem exponentially faster than the best known classical algorithm.[14]

Linear differential equation solving

Dominic Berry proposed a new algorithm for solving linear time dependent differential equations as an extension of the quantum algorithm for solving linear systems of equations. Berry provides an efficient algorithm for solving the full-time evolution under sparse linear differential equations on a quantum computer.[15]

Nonlinear differential equation solving

Two groups proposed[16] efficient algorithms for numerically integrating dissipative nonlinear ordinary differential equations. Liu et al.[17] utilized Carleman linearization technique for second order equations and Lloyd et al.[18] employed a mean field linearization method inspired by nonlinear Schrödinger equation for general order nonlinearities. The resulting linear equations are solved using quantum algorithms for linear differential equations.

Finite element method

The Finite Element Method uses large systems of linear equations to find approximate solutions to various physical and mathematical models. Montanaro and Pallister demonstrate that the HHL algorithm, when applied to certain FEM problems, can achieve a polynomial quantum speedup. They suggest that an exponential speedup is not possible in problems with fixed dimensions, and for which the solution meets certain smoothness conditions.

Quantum speedups for the finite element method are higher for problems which include solutions with higher-order derivatives and large spatial dimensions. For example, problems in many-body dynamics require the solution of equations containing derivatives on orders scaling with the number of bodies, and some problems in computational finance, such as Black-Scholes models, require large spatial dimensions.[19]

Least-squares fitting

Wiebe et al. provide a new quantum algorithm to determine the quality of a least-squares fit in which a continuous function is used to approximate a set of discrete points by extending the quantum algorithm for linear systems of equations. As the number of discrete points increases, the time required to produce a least-squares fit using even a quantum computer running a quantum state tomography algorithm becomes very large. Wiebe et al. find that in many cases, their algorithm can efficiently find a concise approximation of the data points, eliminating the need for the higher-complexity tomography algorithm.[20]

Machine learning and big data analysis

Machine learning is the study of systems that can identify trends in data. Tasks in machine learning frequently involve manipulating and classifying a large volume of data in high-dimensional vector spaces. The runtime of classical machine learning algorithms is limited by a polynomial dependence on both the volume of data and the dimensions of the space. Quantum computers are capable of manipulating high-dimensional vectors using tensor product spaces and thus are well-suited platforms for machine learning algorithms.[21]

The quantum algorithm for linear systems of equations has been applied to a support vector machine, which is an optimized linear or non-linear binary classifier. A support vector machine can be used for supervised machine learning, in which training set of already classified data is available, or unsupervised machine learning, in which all data given to the system is unclassified. Rebentrost et al. show that a quantum support vector machine can be used for big data classification and achieve an exponential speedup over classical computers.[22]

In June 2018, Zhao et al. developed an algorithm for performing Bayesian training of deep neural networks in quantum computers with an exponential speedup over classical training due to the use of the quantum algorithm for linear systems of equations,[6] providing also the first general-purpose implementation of the algorithm to be run in cloud-based quantum computers.[23]

Finance

Proposals for using HHL in finance include solving partial differential equations for the Black–Scholes equation and determining portfolio optimization via a Markowitz solution.[24]

Quantum chemistry

In 2023, Baskaran et al. proposed the use of HHL algorithm to quantum chemistry calculations, via the linearized coupled cluster method (LCC).[25] The connection between the HHL algorithm and the LCC method is due to the fact that the latter can be recast in the form of system of linear equations. A key factor that makes this approach useful for quantum chemistry is that the number of state register qubits is the natural logarithm of the number of excitations, thus offering an exponential suppression in the number of required qubits when compared to variational quantum eigensolver or the quantum phase estimation algorithms. This leads to a 'coexistence across scales', where in a given quantum computing era, HHL-LCC could be applied to much larger systems whereas QPE-CASCI could be employed for smaller molecular systems but with better accuracy in predicting molecular properties. On the algorithmic side, the authors introduce the 'AdaptHHL' approach, which circumvents the need to expend an ~$O(N^3)$ classical overhead associated with fixing a value for the parameter 'c' in the controlled-rotation module of the algorithm.

Critique

Recognizing the importance of the HHL algorithm in the field of *quantum machine learning*, Scott Aaronson[26] analyzes the caveats and factors that could limit the actual quantum advantage of the algorithm.

1. the solution vector, $|b\rangle$, has to be *efficiently* prepared in the quantum state. If the vector is not close to uniform, the state preparation is likely to be costly, and if it takes $O(n^c)$ steps the exponential advantage of HHL would vanish.
2. the QPE phases calls for the generation of the unitary e^{iAt}, and its controlled application. The efficiency of this step depends on the A matrix being sparse and 'well conditioned' (low κ). Otherwise, the application of e^{iAt} would grow as $O(n^c)$ and once again, the algorithm's quantum advantage would vanish.
3. lastly, the vector, $|x\rangle$, is not readily accessible. The HHL algorithm enables learning a 'summary' of the vector, namely the result of measuring the expectation of an operator $\langle x|M|x\rangle$. If actual values of $\vec{x}$ are needed, then HHL would need to be repeated $O(n)$ times, killing the exponential speed-up. However, three ways of avoiding getting the actual values have been proposed: first, if only some properties of the solution are needed;[27] second, if the results are needed only to feed downstream matrix operations; third, if only a sample of the solution is needed.[28]

See also

- Differentiable programming

References

1. Harrow, Aram W; Hassidim, Avinatan; Lloyd, Seth (2008). "Quantum algorithm for linear systems of equations". *Physical Review Letters*. **103** (15): 150502. arXiv:0811.3171 (https://arxiv.org/abs/0811.3171). Bibcode:2009PhRvL.103o0502H (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103o0502H). doi:10.1103/PhysRevLett.103.150502 (https://doi.org/10.1103%2FPhysRevLett.103.150502). PMID 19905613 (https://pubmed.ncbi.nlm.nih.gov/19905613). S2CID 5187993 (https://api.semanticscholar.org/CorpusID:5187993).
2. Johnston, Eric (2019-07-03). *Programming Quantum Computers: Essential Algorithms and Code Samples* (https://books.google.com/books?id=QqegDwAAQBAJ&pg=PA267). O'Reilly Media. p. 267. ISBN 9781492039655.
3. Cai, X.-D; Weedbrook, C; Su, Z.-E; Chen, M.-C; Gu, Mile; Zhu, M.-J; Li, Li; Liu, Nai-Le; Lu, Chao-Yang; Pan, Jian-Wei (2013). "Experimental Quantum Computing to Solve Systems of Linear Equations". *Physical Review Letters*. **110** (23): 230501. arXiv:1302.4310 (https://arxiv.org/abs/1302.4310). Bibcode:2013PhRvL.110w0501C (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110w0501C). doi:10.1103/PhysRevLett.110.230501 (https://doi.org/10.1103%2FPhysRevLett.110.230501). PMID 25167475 (https://pubmed.ncbi.nlm.nih.gov/25167475). S2CID 20427454 (https://api.semanticscholar.org/CorpusID:20427454).
4. Barz, Stefanie; Kassal, Ivan; Ringbauer, Martin; Lipp, Yannick Ole; Dakić, Borivoje; Aspuru-Guzik, Alán; Walther, Philip (2014). "A two-qubit photonic quantum processor and its application to solving systems of linear equations" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4137340). *Scientific Reports*. **4**: 6115. arXiv:1302.1210 (https://arxiv.org/abs/1302.1210). Bibcode:2014NatSR...4E6115B (https://ui.adsabs.harvard.edu/abs/2014NatSR...4E6115B). doi:10.1038/srep06115 (https://doi.org/10.1038%2Fsrep06115). ISSN 2045-2322 (https://search.worldcat.org/issn/2045-2322). PMC 4137340 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4137340). PMID 25135432 (https://pubmed.ncbi.nlm.nih.gov/25135432).

5. Pan, Jian; Cao, Yudong; Yao, Xiwei; Li, Zhaokai; Ju, Chenyong; Peng, Xinhua; Kais, Sabre; Du, Jiangfeng; Du, Jiangfeng (2014). "Experimental realization of quantum algorithm for solving linear systems of equations". *Physical Review A*. **89** (2): 022313. arXiv:1302.1946 (https://arxiv.org/abs/1302.1946). Bibcode:2014PhRvA..89b2313P (https://ui.adsabs.harvard.edu/abs/2014PhRvA..89b2313P). doi:10.1103/PhysRevA.89.022313 (https://doi.org/10.1103%2FPhysRevA.89.022313). S2CID 14303240 (https://api.semanticscholar.org/CorpusID:14303240).
6. Zhao, Zhikuan; Pozas-Kerstjens, Alejandro; Rebentrost, Patrick; Wittek, Peter (2019). "Bayesian Deep Learning on a Quantum Computer". *Quantum Machine Intelligence*. **1** (1–2): 41–51. arXiv:1806.11463 (https://arxiv.org/abs/1806.11463). doi:10.1007/s42484-019-00004-7 (https://doi.org/10.1007%2Fs42484-019-00004-7). S2CID 49554188 (https://api.semanticscholar.org/CorpusID:49554188).
7. Quantum Computer Runs The Most Practically Useful Quantum Algorithm, by Lu and Pan (http://www.2physics.com/2013/06/quantum-computer-runs-most-practically.html).
8. Ambainis, Andris (2010). "Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations". arXiv:1010.4458 (https://arxiv.org/abs/1010.4458) [quant-ph (https://arxiv.org/archive/quant-ph)].
9. Childs, Andrew M.; Kothari, Robin; Somma, Rolando D. (2017). "Quantum Algorithm for Systems of Linear Equations with Exponentially Improved Dependence on Precision". *SIAM Journal on Computing*. **46** (6): 1920–1950. arXiv:1511.02306 (https://arxiv.org/abs/1511.02306). doi:10.1137/16m1087072 (https://doi.org/10.1137%2F16m1087072). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397). S2CID 3834959 (https://api.semanticscholar.org/CorpusID:3834959).
10. Wossnig, Leonard; Zhao, Zhikuan; Prakash, Anupam (2018). "A quantum linear system algorithm for dense matrices". *Physical Review Letters*. **120** (5): 050502. arXiv:1704.06174 (https://arxiv.org/abs/1704.06174). Bibcode:2018PhRvL.120e0502W (https://ui.adsabs.harvard.edu/abs/2018PhRvL.120e0502W). doi:10.1103/PhysRevLett.120.050502 (https://doi.org/10.1103%2FPhysRevLett.120.050502). PMID 29481180 (https://pubmed.ncbi.nlm.nih.gov/29481180). S2CID 3714239 (https://api.semanticscholar.org/CorpusID:3714239).
11. Cai, X. -D; Weedbrook, Christian; Su, Z. -E; Chen, M. -C; Gu, Mile; Zhu, M. -J; Li, L; Liu, N. -L; Lu, Chao-Yang; Pan, Jian-Wei (2013). "Experimental Quantum Computing to Solve Systems of Linear Equations". *Physical Review Letters*. **110** (23): 230501. arXiv:1302.4310 (https://arxiv.org/abs/1302.4310). Bibcode:2013PhRvL.110w0501C (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110w0501C). doi:10.1103/PhysRevLett.110.230501 (https://doi.org/10.1103%2FPhysRevLett.110.230501). PMID 25167475 (https://pubmed.ncbi.nlm.nih.gov/25167475). S2CID 20427454 (https://api.semanticscholar.org/CorpusID:20427454).
12. Jingwei Wen, Xiangyu Kong, Shijie Wei, Bixue Wang, Tao Xin, and Guilu Long (2019). "Experimental realization of quantum algorithms for a linear system inspired by adiabatic quantum computing". Phys. Rev. A **99**, 012320.
13. Subaşı, Yiğit; Somma, Rolando D.; Orsucci, Davide (2019-02-14). "Quantum Algorithms for Systems of Linear Equations Inspired by Adiabatic Quantum Computing". *Physical Review Letters*. **122** (6): 060504. arXiv:1805.10549 (https://arxiv.org/abs/1805.10549). Bibcode:2019PhRvL.122f0504S (https://ui.adsabs.harvard.edu/abs/2019PhRvL.122f0504S). doi:10.1103/physrevlett.122.060504 (https://doi.org/10.1103%2Fphysrevlett.122.060504). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 30822089 (https://pubmed.ncbi.nlm.nih.gov/30822089). S2CID 73493666 (https://api.semanticscholar.org/CorpusID:73493666).
14. Clader, B. D; Jacobs, B. C; Sprouse, C. R (2013). "Preconditioned Quantum Linear System Algorithm". *Physical Review Letters*. **110** (25): 250504. arXiv:1301.2340 (https://arxiv.org/abs/1301.2340). Bibcode:2013PhRvL.110y0504C (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110y0504C). doi:10.1103/PhysRevLett.110.250504 (https://doi.org/10.1103%2FPhysRevLett.110.250504). PMID 23829722 (https://pubmed.ncbi.nlm.nih.gov/23829722). S2CID 33391978 (https://api.semanticscholar.org/CorpusID:33391978).

15. Berry, Dominic W (2010). "High-order quantum algorithm for solving linear differential equations". *Journal of Physics A: Mathematical and Theoretical*. **47** (10): 105301. arXiv:1010.2745 (https://arxiv.org/abs/1010.2745). Bibcode:2014JPhA...47j5301B (https://ui.adsabs.harvard.edu/abs/2014JPhA...47j5301B). doi:10.1088/1751-8113/47/10/105301 (https://doi.org/10.1088%2F1751-8113%2F47%2F10%2F105301). S2CID 17623971 (https://api.semanticscholar.org/CorpusID:17623971).
16. Levy, Max G. (January 5, 2021). "New Quantum Algorithms Finally Crack Nonlinear Equations" (https://www.quantamagazine.org/new-quantum-algorithms-finally-crack-nonlinear-equations-20210105/). *Quanta Magazine*. Retrieved December 31, 2022.
17. Liu, J.P.; Kolden, H.Ø.; Krovi, H.K.; Loureiro, N.F.; Trivisa, K.; Childs, A.M. (2021). "Efficient quantum algorithm for dissipative nonlinear differential equations" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8536387). *PNAS*. **118** (35): e2026805118. arXiv:2011.03185 (https://arxiv.org/abs/2011.03185). Bibcode:2021PNAS..11826805L (https://ui.adsabs.harvard.edu/abs/2021PNAS..11826805L). doi:10.1073/pnas.2026805118 (https://doi.org/10.1073%2Fpnas.2026805118). PMC 8536387 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8536387). PMID 34446548 (https://pubmed.ncbi.nlm.nih.gov/34446548).
18. Lloyd, S.; De Palma, G; Gokler, C.; Kiani, B.; Liu, Z.W.; Marvian, M.; Tennie, F.; Palmer, T. (2020). "Quantum algorithm for nonlinear differential equations". arXiv:2011.06571 (https://arxiv.org/abs/2011.06571) [quant-ph (https://arxiv.org/archive/quant-ph)].
19. Montanaro, Ashley; Pallister, Sam (2016). "Quantum Algorithms and the Finite Element Method". *Physical Review A*. **93** (3): 032324. arXiv:1512.05903 (https://arxiv.org/abs/1512.05903). Bibcode:2016PhRvA..93c2324M (https://ui.adsabs.harvard.edu/abs/2016PhRvA..93c2324M). doi:10.1103/PhysRevA.93.032324 (https://doi.org/10.1103%2FPhysRevA.93.032324). S2CID 44004935 (https://api.semanticscholar.org/CorpusID:44004935).
20. Wiebe, Nathan; Braun, Daniel; Lloyd, Seth (2012). "Quantum Data Fitting". *Physical Review Letters*. **109** (5): 050505. arXiv:1204.5242 (https://arxiv.org/abs/1204.5242). Bibcode:2012PhRvL.109e0505W (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109e0505W). doi:10.1103/PhysRevLett.109.050505 (https://doi.org/10.1103%2FPhysRevLett.109.050505). PMID 23006156 (https://pubmed.ncbi.nlm.nih.gov/23006156). S2CID 118439810 (https://api.semanticscholar.org/CorpusID:118439810).
21. Lloyd, Seth; Mohseni, Masoud; Rebentrost, Patrick (2013). "Quantum algorithms for supervised and unsupervised machine learning". arXiv:1307.0411 (https://arxiv.org/abs/1307.0411) [quant-ph (https://arxiv.org/archive/quant-ph)].
22. Rebentrost, Patrick; Mohseni, Masoud; Lloyd, Seth (2013). "Quantum support vector machine for big feature and big data classification". arXiv:1307.0471v2 (https://arxiv.org/abs/1307.0471v2) [quant-ph (https://arxiv.org/archive/quant-ph)].
23. "apozas/bayesian-dl-quantum" (https://gitlab.com/apozas/bayesian-dl-quantum). *GitLab*. Retrieved 30 October 2018.
24. Jacquier, Antoine (2022-10-31). *Quantum Machine Learning and Optimisation in Finance: On the Road to Quantum Advantage* (https://books.google.com/books?id=22SXEAAAQBAJ&pg=PA349). Packt. p. 349. ISBN 9781801817875.
25. Baskaran, N (2023). "Adapting the Harrow-Hassidim-Lloyd algorithm to quantum many-body theory" (https://doi.org/10.1103%2FPhysRevResearch.5.043113). *Physical Review Research*. **5** (4): 043113. Bibcode:2023PhRvR...5d3113B (https://ui.adsabs.harvard.edu/abs/2023PhRvR...5d3113B). doi:10.1103/PhysRevResearch.5.043113 (https://doi.org/10.1103%2FPhysRevResearch.5.043113).
26. Aaronson, Scott (2015). "Read the fine print" (https://www.nature.com/articles/nphys3272). *Nature Physics*. **11** (4): 291–293. Bibcode:2015NatPh..11..291A (https://ui.adsabs.harvard.edu/abs/2015NatPh..11..291A). doi:10.1038/nphys3272 (https://doi.org/10.1038%2Fnphys3272). S2CID 122167250 (https://api.semanticscholar.org/CorpusID:122167250). Retrieved 2023-05-09.

27. Schuld, Maria (2018). *Supervised Learning with Quantum Computers* (https://books.google.com/books?id=1zpsDwAAQBAJ&pg=PA218). Springer Publishing. p. 218. ISBN 9783319964249.
28. Schuld, Maria (2018). *Supervised Learning with Quantum Computers* (https://books.google.com/books?id=1zpsDwAAQBAJ&pg=PA219). Springer Publishing. p. 219. ISBN 9783319964249.

Retrieved from "https://en.wikipedia.org/w/index.php?title=HHL_algorithm&oldid=1239006789"

WIKIPEDIA
The Free Encyclopedia

Hidden subgroup problem

The **hidden subgroup problem** (**HSP**) is a topic of research in mathematics and theoretical computer science. The framework captures problems such as factoring, discrete logarithm, graph isomorphism, and the shortest vector problem. This makes it especially important in the theory of quantum computing because Shor's algorithms for factoring and finding discrete logarithms in quantum computing are instances of the hidden subgroup problem for finite abelian groups, while the other problems correspond to finite groups that are not abelian.

Problem statement

Given a group G, a subgroup $H \leq G$, and a set X, we say a function $f : G \to X$ **hides** the subgroup H if for all $g_1, g_2 \in G, f(g_1) = f(g_2)$ if and only if $g_1 H = g_2 H$. Equivalently, f is constant on each coset of H, while it is different between the different cosets of H.

Hidden subgroup problem: Let G be a group, X a finite set, and $f : G \to X$ a function that hides a subgroup $H \leq G$. The function f is given via an oracle, which uses $O(\log |G| + \log |X|)$ bits. Using information gained from evaluations of f via its oracle, determine a generating set for H.

A special case is when X is a group and f is a group homomorphism in which case H corresponds to the kernel of f.

Motivation

The hidden subgroup problem is especially important in the theory of quantum computing for the following reasons.

- Shor's algorithm for factoring and for finding discrete logarithms (as well as several of its extensions) relies on the ability of quantum computers to solve the HSP for finite abelian groups.
- The existence of efficient quantum algorithms for HSPs for certain non-abelian groups would imply efficient quantum algorithms for two major problems: the graph isomorphism problem and certain shortest vector problems (SVPs) in lattices. More precisely, an efficient quantum algorithm for the HSP for the symmetric group would give a quantum algorithm for the graph isomorphism.[1] An efficient quantum algorithm for the HSP for the dihedral group would give a quantum algorithm for the $\mathbf{poly}(n)$ unique SVP.[2]

Algorithms

There is an efficient quantum algorithm for solving HSP over finite abelian groups in time polynomial in $\log |G|$. For arbitrary groups, it is known that the hidden subgroup problem is solvable using a polynomial number of evaluations of the oracle.[3] However, the circuits that implement this may be exponential in $\log |G|$, making the algorithm not efficient overall; efficient algorithms must be

polynomial in the number of oracle evaluations and running time. The existence of such an algorithm for arbitrary groups is open. Quantum polynomial time algorithms exist for certain subclasses of groups, such as semi-direct products of some abelian groups.

Algorithm for abelian groups

The algorithm for abelian groups uses representations, i.e. homomorphisms from G to $\mathrm{GL}_k(\mathbb{C})$, the general linear group over the complex numbers. A representation is irreducible if it cannot be expressed as the direct product of two or more representations of G. For an abelian group, all the irreducible representations are the characters, which are the representations of dimension one; there are no irreducible representations of larger dimension for abelian groups.

Defining the quantum fourier transform

The quantum fourier transform can be defined in terms of $\mathbf{Z}_N$, the additive cyclic group of order N. Introducing the character

$$\chi_j(k) = \omega_N^{jk} = e^{2\pi i \frac{jk}{N}},$$

the quantum fourier transform has the definition of

$$F_N|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N} \chi_j(k)|k\rangle.$$

Furthermore we define $|\chi_j\rangle = F_N|j\rangle$. Any finite abelian group can be written as the direct product of multiple cyclic groups $\mathbf{Z}_{N_1} \times \mathbf{Z}_{N_2} \times \ldots \times \mathbf{Z}_{N_m}$. On a quantum computer, this is represented as the tensor product of multiple registers of dimensions $N_1, N_2, \ldots, N_m$ respectively, and the overall quantum fourier transform is $F_{N_1} \otimes F_{N_2} \otimes \ldots \otimes F_{N_m}$.

Procedure

The set of characters of G forms a group $\widehat{G}$ called the dual group of G. We also have a subgroup $H^\perp \leq \widehat{G}$ of size $|G|/|H|$ defined by

$$H^\perp = \{\chi_g : \chi_g(h) = 1 \text{ for all } h \in H\}$$

For each iteration of the algorithm, the quantum circuit outputs a element $g \in G$ corresponding to a character $\chi_g \in H^\perp$, and since $\chi_g(h) = 1$ for all $h \in H$, it helps to pin down what H is.

The algorithm is as follows:

1. Start with the state $|0\rangle|0\rangle$, where the left register's basis states are each element of G, and the right register's basis states are each element of X.
2. Create a superposition among the basis states of G in the left register, leaving the state $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$.
3. Query the function f. The state afterwards is $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$.

4. Measure the output register. This gives some $f(s)$ for some $s \in G$, and collapses the state to $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |s+h\rangle |f(s)\rangle$ because f has the same value for each element of the coset $s+H$. We discard the output register to get $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |s+h\rangle$.
5. Perform the quantum fourier transform, getting the state $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |\chi_{s+h}\rangle$.
6. This state is equal to $\sqrt{\frac{|H|}{|G|}} \sum_{\chi_g \in H^\perp} \chi_g(s)|g\rangle$, which can be measured to learn information about H.
7. Repeat until H (or a generating set for H) is determined.

The state in step 5 is equal to the state in step 6 because of the following:

$$\begin{aligned}
\frac{1}{\sqrt{|H|}} \sum_{h \in H} |\chi_{s+h}\rangle &= \frac{1}{\sqrt{|H||G|}} \sum_{h \in H} \sum_{g \in G} \chi_{s+h}(g)|g\rangle \\
&= \frac{1}{\sqrt{|H||G|}} \sum_{g \in G} \chi_s(g) \sum_{h \in H} \chi_h(g)|g\rangle \\
&= \frac{1}{\sqrt{|H||G|}} \sum_{g \in G} \chi_g(s) \left(\sum_{h \in H} \chi_g(h) \right) |g\rangle \\
&= \sqrt{\frac{|H|}{|G|}} \sum_{\chi_g \in H^\perp} \chi_g(s)|g\rangle
\end{aligned}$$

For the last equality, we use the following identity:

Theorem —

$$\sum_{h \in H} \chi_g(h) = \begin{cases} |H| & \chi_g \in H^\perp \\ 0 & \chi_g \notin H^\perp \end{cases}$$

Proof

This can be derived from the orthogonality of characters. The characters of G form an orthonormal basis:

$$\frac{1}{|H|} \sum_{h \in H} \chi_g(h) \chi_{g'}(h) = \begin{cases} 1 & g = g' \\ 0 & g \neq g' \end{cases}$$

We let $\chi_{g'}$ be the trivial representation, which maps all inputs to 1, to get

$$\sum_{h \in H} \chi_g(h) = \begin{cases} |H| & g \text{ is trivial} \\ 0 & g \text{ is not trivial} \end{cases}$$

Since the summation is done over H, χ_g also being trivial only matters for if it is trivial over H; that is, if $\chi_g \in H^\perp$. Thus, we know that the summation will result in $|H|$ if $\chi_g \in H^\perp$ and will result in 0 if $\chi_g \notin H^\perp$.

Each measurement of the final state will result in some information gained about H since we know that $\chi_g(h) = 1$ for all $h \in H$. H, or a generating set for H, will be found after a polynomial number of measurements. The size of a generating set will be logarithmically small compared to the size of G. Let T denote a generating set for H, meaning $\langle T \rangle = H$. The size of the subgroup generated by T will at least be doubled when a new element $t \notin T$ is added to it, because H and $t + H$ are disjoint and because $H \cup t + H \subseteq \langle \{t\} \cup T \rangle$. Therefore, the size of a generating set $|T|$ satisfies

$$|T| \leq \log |H| \leq \log |G|$$

Thus a generating set for H will be able to be obtained in polynomial time even if G is exponential in size.

Instances

Many algorithms where quantum speedups occur in quantum computing are instances of the hidden subgroup problem. The following list outlines important instances of the HSP, and whether or not they are solvable.

Problem	Quantum Algorithm	Abelian?	Polynomial time solution?
Deutsch's problem	Deutsch's algorithm; Deutsch-Jozsa algorithm	Yes	Yes
Simon's problem	Simon's algorithm	Yes	Yes
Order finding	Shor's order finding algorithm	Yes	Yes
Discrete logarithm	Shor's algorithm § Discrete logarithms	Yes	Yes
Period finding	Shor's algorithm	Yes	Yes
Abelian stabilizer	Kitaev's algorithm[4]	Yes	Yes
Graph Isomorphism	None	No	No
Shortest vector problem	None	No	No

See also

- Hidden shift problem

- Pontryagin duality

References

1. Mark Ettinger; Peter Høyer (1999). "A quantum observable for the graph isomorphism problem". arXiv:quant-ph/9901029 (https://arxiv.org/abs/quant-ph/9901029).
2. Oded Regev (2003). "Quantum computation and lattice problems". arXiv:cs/0304005 (https://arxiv.org/abs/cs/0304005).
3. Mark Ettinger; Peter Hoyer; Emanuel Knill (2004). "The quantum query complexity of the hidden subgroup problem is polynomial". *Information Processing Letters*. **91**: 43–48. arXiv:quant-ph/0401083 (https://arxiv.org/abs/quant-ph/0401083). Bibcode:2004quant.ph..1083E (https://ui.adsabs.harvard.edu/abs/2004quant.ph..1083E). doi:10.1016/j.ipl.2004.01.024 (https://doi.org/10.1016%2Fj.ipl.2004.01.024). S2CID 5520617 (https://api.semanticscholar.org/CorpusID:5520617).
4. Kitaev, Alexei (November 20, 1995). "Quantum measurements and the Abelian Stabilizer Problem". arXiv:quant-ph/9511026 (https://arxiv.org/abs/quant-ph/9511026).

External links

- Richard Jozsa: Quantum factoring, discrete logarithms and the hidden subgroup problem (https://arxiv.org/abs/quant-ph/0012084)
- Chris Lomont: The Hidden Subgroup Problem - Review and Open Problems (https://arxiv.org/abs/quant-ph/0411037)
- Hidden subgroup problem on arxiv.org (http://xstructure.inr.ac.ru/x-bin/theme2.py?arxiv=quant-ph&level=1&index1=14486)
- Complete implementation of Shor's algorithm for finding discrete logarithms with Classiq (https://short.classiq.io/discrete_log)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Hidden_subgroup_problem&oldid=1241283035"

WIKIPEDIA
The Free Encyclopedia

Quantum annealing

Quantum annealing (**QA**) is an optimization process for finding the global minimum of a given objective function over a given set of candidate solutions (candidate states), by a process using quantum fluctuations. Quantum annealing is used mainly for problems where the search space is discrete (combinatorial optimization problems) with many local minima; such as finding[1] the ground state of a spin glass or the traveling salesman problem. The term "quantum annealing" was first proposed in 1988 by B. Apolloni, N. Cesa Bianchi and D. De Falco as a quantum-inspired classical algorithm.[2][3] It was formulated in its present form by T. Kadowaki and H. Nishimori (ja) in 1998[4] though an imaginary-time variant without quantum coherence had been discussed by A. B. Finnila, M. A. Gomez, C. Sebenik and J. D. Doll in 1994.[5]

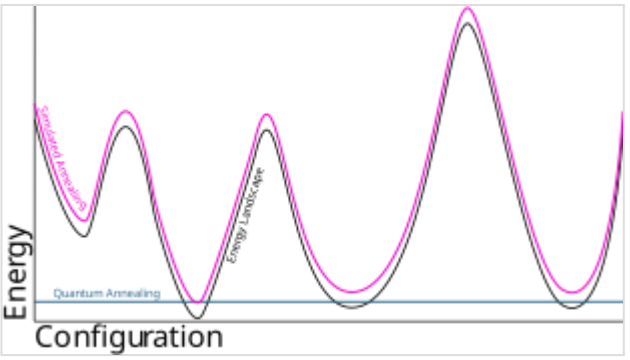
Quantum annealing starts from a quantum-mechanical superposition of all possible states (candidate states) with equal weights. Then the system evolves following the time-dependent Schrödinger equation, a natural quantum-mechanical evolution of physical systems. The amplitudes of all candidate states keep changing, realizing a quantum parallelism, according to the time-dependent strength of the transverse field, which causes quantum tunneling between states or essentially tunneling through peaks. If the rate of change of the transverse field is slow enough, the system stays close to the ground state of the instantaneous Hamiltonian (also see adiabatic quantum computation).[6] If the rate of change of the transverse field is accelerated, the system may leave the ground state temporarily but produce a higher likelihood of concluding in the ground state of the final problem Hamiltonian, i.e., Diabatic quantum computation.[7][8] The transverse field is finally switched off, and the system is expected to have reached the ground state of the classical Ising model that corresponds to the solution to the original optimization problem. An experimental demonstration of the success of quantum annealing for random magnets was reported immediately after the initial theoretical proposal.[9] Quantum annealing has also been proven to provide a fast Grover oracle for the square-root speedup in solving many NP-complete problems.[10]

Comparison to Simulated Annealing

Quantum annealing can be compared to simulated annealing, whose "temperature" parameter plays a similar role to QA's tunneling field strength. In simulated annealing, the temperature determines the probability of moving to a state of higher "energy" from a single current state. In quantum annealing, the strength of transverse field determines the quantum-mechanical probability to change the amplitudes of all states in parallel. Analytical[11] and numerical[12] evidence suggests that quantum annealing outperforms simulated annealing under certain conditions (see[13] for a careful analysis, and,[14] for a fully solvable model of quantum annealing to arbitrary target Hamiltonian and comparison of different computation approaches).

Quantum mechanics: analogy and advantage

The tunneling field is basically a kinetic energy term that does not commute with the classical potential energy part of the original glass. The whole process can be simulated in a computer using quantum Monte Carlo (or other stochastic technique), and thus obtain a heuristic algorithm for finding the ground state of the classical glass.



Quantum Annealing (blue line) efficiently traverses energy landscapes by leveraging quantum tunneling to find the global minimum. Quantum annealing offers a significant performance advantage over Simulated Annealing (magenta line), unlocking the potential to solve massive optimization problems previously thought to be impossible.

In the case of annealing a purely mathematical *objective function*, one may consider the variables in the problem to be classical degrees of freedom, and the cost functions to be the potential energy function (classical Hamiltonian). Then a suitable term consisting of non-commuting variable(s) (i.e. variables that have non-zero commutator with the variables of the original mathematical problem) has to be introduced artificially in the Hamiltonian to play the role of the tunneling field (kinetic part). Then one may carry out the simulation with the quantum Hamiltonian thus constructed (the original function + non-commuting part) just as described above. Here, there is a choice in selecting the non-commuting term and the efficiency of annealing may depend on that.

It has been demonstrated experimentally as well as theoretically, that quantum annealing can indeed outperform thermal annealing (simulated annealing) in certain cases, especially where the potential energy (cost) landscape consists of very high but thin barriers surrounding shallow local minima.[15] Since thermal transition probabilities (proportional to $e^{-\frac{\Delta}{k_B T}}$, with T the temperature and k_B the Boltzmann constant) depend only on the height Δ of the barriers, for very high barriers, it is extremely difficult for thermal fluctuations to get the system out from such local minima. However, as argued earlier in 1989 by Ray, Chakrabarti & Chakrabarti,[1] the quantum tunneling probability through the same barrier (considered in isolation) depends not only on the height Δ of the barrier, but also on its width w and is approximately given by $e^{-\frac{\sqrt{\Delta} w}{\Gamma}}$, where Γ is the tunneling field.[16] This additional handle through the width w, in presence of quantum tunneling, can be of major help: If the barriers are thin enough (i.e. $w \ll \sqrt{\Delta}$), quantum fluctuations can surely bring the system out of the shallow local minima. For an N-spin glass, the barrier height Δ becomes of order N. For constant value of w one gets τ proportional to $e^{\sqrt{N}}$ for the annealing time (instead of τ proportional to e^{N} for thermal annealing), while τ can even become N-independent for cases where w decreases as $1/\sqrt{N}$.[17][18]

It is speculated that in a quantum computer, such simulations would be much more efficient and exact than that done in a classical computer, because it can perform the tunneling directly, rather than needing to add it by hand. Moreover, it may be able to do this without the tight error controls needed to harness the quantum entanglement used in more traditional quantum algorithms. Some confirmation of this is found in exactly solvable models.[19][20]

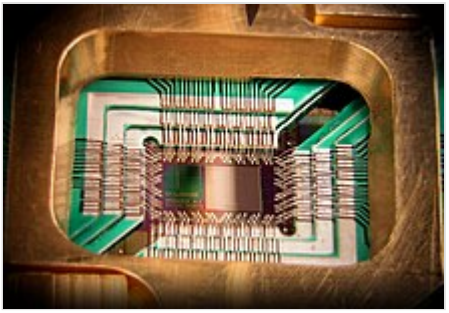
Timeline of ideas related to quantum annealing in Ising spin glasses:

- 1989 Idea was presented that quantum fluctuations could help explore rugged energy landscapes of the classical Ising spin glasses by escaping from local minima (having tall but

thin barriers) using tunneling;[1]
- 1998 Formulation of quantum annealing and numerical test demonstrating its advantages in Ising glass systems;[4]
- 1999 First experimental demonstration of quantum annealing in LiHoYF Ising glass magnets;[21]
- 2011 Superconducting-circuit quantum annealing machine built and marketed by D-Wave Systems.[22]

D-Wave implementations

In 2011, D-Wave Systems announced the first commercial quantum annealer on the market by the name D-Wave One and published a paper in Nature on its performance.[22] The company claims this system uses a 128 qubit processor chipset.[23] On May 25, 2011, D-Wave announced that Lockheed Martin Corporation entered into an agreement to purchase a D-Wave One system.[24] On October 28, 2011 USC's Information Sciences Institute took delivery of Lockheed's D-Wave One.



Photograph of a chip constructed by D-Wave Systems, mounted and wire-bonded in a sample holder. The D-Wave One's processor is designed to use 128 superconducting logic elements that exhibit controllable and tunable coupling to perform operations.

In May 2013 it was announced that a consortium of Google, NASA Ames and the non-profit Universities Space Research Association purchased an adiabatic quantum computer from D-Wave Systems with 512 qubits.[25][26] An extensive study of its performance as quantum annealer, compared to some classical annealing algorithms, is already available.[27]

In June 2014, D-Wave announced a new quantum applications ecosystem with computational finance firm 1QB Information Technologies (1QBit) and cancer research group DNA-SEQ to focus on solving real-world problems with quantum hardware.[28] As the first company dedicated to producing software applications for commercially available quantum computers, 1QBit's research and development arm has focused on D-Wave's quantum annealing processors and has successfully demonstrated that these processors are suitable for solving real-world applications.[29]

With demonstrations of entanglement published,[30] the question of whether or not the D-Wave machine can demonstrate quantum speedup over all classical computers remains unanswered. A study published in Science in June 2014, described as "likely the most thorough and precise study that has been done on the performance of the D-Wave machine"[31] and "the fairest comparison yet", attempted to define and measure quantum speedup. Several definitions were put forward as some may be unverifiable by empirical tests, while others, though falsified, would nonetheless allow for the existence of performance advantages. The study found that the D-Wave chip "produced no quantum speedup" and did not rule out the possibility in future tests.[32] The researchers, led by Matthias Troyer at the Swiss Federal Institute of Technology, found "no quantum speedup" across the entire range of their tests, and only inconclusive results when looking at subsets of the tests. Their work illustrated "the subtle nature of the quantum speedup question". Further work[33] has advanced understanding of these test metrics and their reliance on equilibrated systems, thereby missing any signatures of advantage due to quantum dynamics.

There are many open questions regarding quantum speedup. The ETH reference in the previous section is just for one class of benchmark problems. Potentially there may be other classes of problems where quantum speedup might occur. Researchers at Google, LANL, USC, Texas A&M, and D-Wave are working to find such problem classes.[34]

In December 2015, Google announced that the D-Wave 2X outperforms both simulated annealing and Quantum Monte Carlo by up to a factor of 100,000,000 on a set of hard optimization problems.[35]

D-Wave's architecture differs from traditional quantum computers. It is not known to be polynomially equivalent to a universal quantum computer and, in particular, cannot execute Shor's algorithm because Shor's algorithm is not a hillclimbing process. Shor's algorithm requires a universal quantum computer. During the Qubits 2021 conference held by D-Wave, it was announced[36] that the company is developing their first universal quantum computers, capable of running Shor's algorithm in addition to other gate-model algorithms such as QAOA and VQE.

"A cross-disciplinary introduction to quantum annealing-based algorithms" [37] presents an introduction to combinatorial optimization (NP-hard) problems, the general structure of quantum annealing-based algorithms and two examples of this kind of algorithms for solving instances of the max-SAT and Minimum Multicut problems, together with an overview of the quantum annealing systems manufactured by D-Wave Systems. Hybrid quantum-classic algorithms for large-scale discrete-continuous optimization problems were reported to illustrate the quantum advantage.[38][39]

References

1. Ray, P.; Chakrabarti, B. K.; Chakrabarti, A. (1989). "Sherrington-Kirkpatrick model in a transverse field: Absence of replica symmetry breaking due to quantum fluctuations". *Physical Review B*. **39** (16): 11828–11832. Bibcode:1989PhRvB..3911828R (https://ui.adsabs.harvard.edu/abs/1989PhRvB..3911828R). doi:10.1103/PhysRevB.39.11828 (https://doi.org/10.1103%2FPhysRevB.39.11828). PMID 9948016 (https://pubmed.ncbi.nlm.nih.gov/9948016).
2. Apolloni, Bruno; Cesa-Bianchi, Nicolo; De Falco, Diego (July 1988). "A numerical implementation of quantum annealing" (https://www.researchgate.net/publication/250309136). Stochastic Processes, Physics and Geometry, Proceedings of the Ascona-Locarno Conference.
3. Apolloni, Bruno; Carvalho, Maria C.; De Falco, Diego (1989). "Quantum stochastic optimization" (https://doi.org/10.1016%2F0304-4149%2889%2990040-9). *Stoc. Proc. Appl.* **33** (2): 233–244. doi:10.1016/0304-4149(89)90040-9 (https://doi.org/10.1016%2F0304-4149%2889%2990040-9).
4. Kadowaki, T.; Nishimori, H. (1998). "Quantum annealing in the transverse Ising model" (https://archive.today/20130811142150/http://pre.aps.org/abstract/PRE/v58/i5/p5355_1). *Phys. Rev. E*. **58** (5): 5355. arXiv:cond-mat/9804280 (https://arxiv.org/abs/cond-mat/9804280). Bibcode:1998PhRvE..58.5355K (https://ui.adsabs.harvard.edu/abs/1998PhRvE..58.5355K). doi:10.1103/PhysRevE.58.5355 (https://doi.org/10.1103%2FPhysRevE.58.5355). S2CID 36114913 (https://api.semanticscholar.org/CorpusID:36114913). Archived from the original (http://pre.aps.org/abstract/PRE/v58/i5/p5355_1) on 2013-08-11.

5. Finnila, A.B.; Gomez, M.A.; Sebenik, C.; Stenson, C.; Doll, J.D. (1994). "Quantum annealing: A new method for minimizing multidimensional functions". *Chemical Physics Letters*. **219** (5–6): 343–348. arXiv:chem-ph/9404003 (https://arxiv.org/abs/chem-ph/9404003). Bibcode:1994CPL...219..343F (https://ui.adsabs.harvard.edu/abs/1994CPL...219..343F). doi:10.1016/0009-2614(94)00117-0 (https://doi.org/10.1016%2F0009-2614%2894%2900117-0). S2CID 97302385 (https://api.semanticscholar.org/CorpusID:97302385).
6. Farhi, E.; Goldstone, J.; Gutmann, S.; Lapan, J.; Ludgren, A.; Preda, D. (2001). "A Quantum adiabatic evolution algorithm applied to random instances of an NP-Complete problem" (https://www.science.org/doi/10.1126/science.1057726). *Science*. **292** (5516): 472–5. arXiv:quant-ph/0104129 (https://arxiv.org/abs/quant-ph/0104129). Bibcode:2001Sci...292..472F (https://ui.adsabs.harvard.edu/abs/2001Sci...292..472F). doi:10.1126/science.1057726 (https://doi.org/10.1126%2Fscience.1057726). PMID 11313487 (https://pubmed.ncbi.nlm.nih.gov/11313487). S2CID 10132718 (https://api.semanticscholar.org/CorpusID:10132718).
7. Crosson, Elizabeth; Farhi, Edward; Cedric Yen-Yu Lin; Lin, Han-Hsuan; Shor, Peter (2014). "Different Strategies for Optimization Using the Quantum Adiabatic Algorithm". arXiv:1401.7320 (https://arxiv.org/abs/1401.7320) [quant-ph (https://arxiv.org/archive/quant-ph)].
8. Muthukrishnan, Siddharth; Albash, Tameem; Lidar, Daniel A. (2015). "When Diabatic Trumps Adiabatic in Quantum Optimization". arXiv:1505.01249 (https://arxiv.org/abs/1505.01249) [quant-ph (https://arxiv.org/archive/quant-ph)].
9. Brooke, J.; Bitko, D.; Rosenbaum, T. F.; Aeppli, G. (1999). "Quantum annealing of a disordered magnet" (https://www.science.org/doi/10.1126/science.284.5415.779). *Science*. **284** (5415): 779–81. arXiv:cond-mat/0105238 (https://arxiv.org/abs/cond-mat/0105238). Bibcode:1999Sci...284..779B (https://ui.adsabs.harvard.edu/abs/1999Sci...284..779B). doi:10.1126/science.284.5415.779 (https://doi.org/10.1126%2Fscience.284.5415.779). PMID 10221904 (https://pubmed.ncbi.nlm.nih.gov/10221904). S2CID 37564720 (https://api.semanticscholar.org/CorpusID:37564720).
10. Sinitsyn, N.; Yan, B. (2023). "Topologically protected Grover's oracle for the partition problem". *Physical Review A*. **108** (2): 022412. arXiv:2304.10488 (https://arxiv.org/abs/2304.10488). Bibcode:2023PhRvA.108b2412S (https://ui.adsabs.harvard.edu/abs/2023PhRvA.108b2412S). doi:10.1103/PhysRevA.108.022412 (https://doi.org/10.1103%2FPhysRevA.108.022412). S2CID 258236417 (https://api.semanticscholar.org/CorpusID:258236417).
11. Morita, Satoshi; Nishimori, Hidetoshi (2008). "Mathematical foundation of quantum annealing". *Journal of Mathematical Physics*. **49** (12): 125210. arXiv:0806.1859 (https://arxiv.org/abs/0806.1859). Bibcode:2008JMP....49l5210M (https://ui.adsabs.harvard.edu/abs/2008JMP....49l5210M). doi:10.1063/1.2995837 (https://doi.org/10.1063%2F1.2995837). S2CID 13992889 (https://api.semanticscholar.org/CorpusID:13992889).
12. Santoro, Giuseppe E. & Tosatti, Erio (18 August 2006). "Optimization using quantum mechanics: quantum annealing through adiabatic evolution" (http://iopscience.iop.org/0305-4470/39/36/R01). *Journal of Physics A*. **39** (36): R393–R431. Bibcode:2006JPhA...39R.393S (https://ui.adsabs.harvard.edu/abs/2006JPhA...39R.393S). doi:10.1088/0305-4470/39/36/R01 (https://doi.org/10.1088%2F0305-4470%2F39%2F36%2FR01). S2CID 116931586 (https://api.semanticscholar.org/CorpusID:116931586).
13. Heim, B.; Rønnow, T. F.; Isakov, S. V.; Troyer, M. (2015). "Quantum versus classical annealing of Ising spin glasses" (https://doi.org/10.1126%2Fscience.aaa4170). *Science*. **348** (6231): 215–217. arXiv:1411.5693 (https://arxiv.org/abs/1411.5693). Bibcode:2015Sci...348..215H (https://ui.adsabs.harvard.edu/abs/2015Sci...348..215H). doi:10.1126/science.aaa4170 (https://doi.org/10.1126%2Fscience.aaa4170). PMID 25765071 (https://pubmed.ncbi.nlm.nih.gov/25765071).

14. Yan, B.; Sinitsyn, N. A. (2022). "Analytical solution for nonadiabatic quantum annealing to arbitrary Ising spin Hamiltonian" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9038765). *Nature Communications*. **13** (1): 2212. arXiv:2110.12354 (https://arxiv.org/abs/2110.12354). Bibcode:2022NatCo..13.2212Y (https://ui.adsabs.harvard.edu/abs/2022NatCo..13.2212Y). doi:10.1038/s41467-022-29887-0 (https://doi.org/10.1038%2Fs41467-022-29887-0). PMC 9038765 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9038765). PMID 35468917 (https://pubmed.ncbi.nlm.nih.gov/35468917). S2CID 248389790 (https://api.semanticscholar.org/CorpusID:248389790).
15. "Local Maxima and Minima, and, Absolute Maxima and Minima" (http://mathonline.wikidot.com/local-maxima-and-minima-and-absolute-maxima-and-minima). *Mathonline*.
16. Das, A.; Chakrabarti, B. K. & Stinchcombe, R. B. (2005). "Quantum annealing in a kinetically constrained system" (https://archive.today/20140113104409/http://pre.aps.org/abstract/PRE/v72/i2/e026701). *Phys. Rev. E*. **72** (2): 026701. arXiv:cond-mat/0502167 (https://arxiv.org/abs/cond-mat/0502167). Bibcode:2005PhRvE..72b6701D (https://ui.adsabs.harvard.edu/abs/2005PhRvE..72b6701D). doi:10.1103/PhysRevE.72.026701 (https://doi.org/10.1103%2FPhysRevE.72.026701). PMID 16196745 (https://pubmed.ncbi.nlm.nih.gov/16196745). S2CID 16466621 (https://api.semanticscholar.org/CorpusID:16466621). Archived from the original (http://pre.aps.org/abstract/PRE/v72/i2/e026701) on 2014-01-13.
17. See e.g., Mukherjee, S. & Chakrabarti, B. K. (2015). "Multivariable Optimization: Quantum Annealing & Computation". *Eur. Phys. J.* **224** (1): 17–24. arXiv:1408.3262 (https://arxiv.org/abs/1408.3262). Bibcode:2015EPJST.224...17M (https://ui.adsabs.harvard.edu/abs/2015EPJST.224...17M). doi:10.1140/epjst/e2015-02339-y (https://doi.org/10.1140%2Fepjst%2Fe2015-02339-y). S2CID 118525494 (https://api.semanticscholar.org/CorpusID:118525494).
18. Das, A.; Chakrabarti, B. K. (2008). "Quantum Annealing and Analog Quantum Computation". *Rev. Mod. Phys.* **80** (3): 1061–1081. arXiv:0801.2193 (https://arxiv.org/abs/0801.2193). Bibcode:2008RvMP...80.1061D (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1061D). CiteSeerX 10.1.1.563.9990 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.563.9990). doi:10.1103/RevModPhys.80.1061 (https://doi.org/10.1103%2FRevModPhys.80.1061). S2CID 14255125 (https://api.semanticscholar.org/CorpusID:14255125).
19. Li, F.; Chernyak, V. Y. & Sinitsyn, N. A. (2018). "Quantum annealing and thermalization: insights from integrability". *Physical Review Letters*. **121** (19): 190601. arXiv:1804.00371 (https://arxiv.org/abs/1804.00371). Bibcode:2018arXiv180400371L (https://ui.adsabs.harvard.edu/abs/2018arXiv180400371L). doi:10.1103/PhysRevLett.121.190601 (https://doi.org/10.1103%2FPhysRevLett.121.190601). PMID 30468584 (https://pubmed.ncbi.nlm.nih.gov/30468584). S2CID 53594139 (https://api.semanticscholar.org/CorpusID:53594139).
20. Yan, B.; Sinitsyn, N. A. (2022). "Analytical solution for nonadiabatic quantum annealing to arbitrary Ising spin Hamiltonian" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9038765). *Nature Communications*. **13** (1): 2212. arXiv:2110.12354 (https://arxiv.org/abs/2110.12354). Bibcode:2022NatCo..13.2212Y (https://ui.adsabs.harvard.edu/abs/2022NatCo..13.2212Y). doi:10.1038/s41467-022-29887-0 (https://doi.org/10.1038%2Fs41467-022-29887-0). PMC 9038765 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9038765). PMID 35468917 (https://pubmed.ncbi.nlm.nih.gov/35468917). S2CID 248389790 (https://api.semanticscholar.org/CorpusID:248389790).
21. Brooke, J.; Bitko, D.; Rosenbaum, T. F. & Aeppli, G. (30 April 1999). "Quantum Annealing of a Disordered Magnet" (https://authors.library.caltech.edu/46977/). *Science*. **284** (5415): 779–781. arXiv:cond-mat/0105238 (https://arxiv.org/abs/cond-mat/0105238). Bibcode:1999Sci...284..779B (https://ui.adsabs.harvard.edu/abs/1999Sci...284..779B). doi:10.1126/science.284.5415.779 (https://doi.org/10.1126%2Fscience.284.5415.779). PMID 10221904 (https://pubmed.ncbi.nlm.nih.gov/10221904). S2CID 37564720 (https://api.semanticscholar.org/CorpusID:37564720).

22. Johnson, M. W.; Amin, M. H. S.; Gildert, S.; et al. (2011). "Quantum annealing with manufactured spins" (http://www.nature.com/nature/journal/v473/n7346/abs/nature10012.html). *Nature*. **473** (7346): 194–8. Bibcode:2011Natur.473..194J (https://ui.adsabs.harvard.edu/abs/2011Natur.473..194J). doi:10.1038/nature10012 (https://doi.org/10.1038%2Fnature10012). PMID 21562559 (https://pubmed.ncbi.nlm.nih.gov/21562559). S2CID 205224761 (https://api.semanticscholar.org/CorpusID:205224761).
23. "Learning to program the D-Wave One" (https://web.archive.org/web/20110723043401/http://dwave.wordpress.com/2011/05/11/learning-to-program-the-d-wave-one/). *D-Wave Systems blog*. Archived from the original (http://dwave.wordpress.com/2011/05/11/learning-to-program-the-d-wave-one/) on July 23, 2011. Retrieved 11 May 2011.
24. "D-Wave Systems sells its first Quantum Computing System to Lockheed Martin Corporation" (https://web.archive.org/web/20110723052206/http://www.dwavesys.com/en/pressreleases.html). *D-Wave*. 2011-05-25. Archived from the original (http://www.dwavesys.com/en/pressreleases.html#lm_2011) on July 23, 2011. Retrieved 2011-05-30.
25. Jones, N. (2013). "Google and NASA snap up quantum computer" (http://www.nature.com/news/google-and-nasa-snap-up-quantum-computer-1.12999). *Nature News*. doi:10.1038/nature.2013.12999 (https://doi.org/10.1038%2Fnature.2013.12999). S2CID 57405432 (https://api.semanticscholar.org/CorpusID:57405432).
26. Smelyanskiy, Vadim N.; Rieffel, Eleanor G.; Knysh, Sergey I.; Williams, Colin P.; Johnson, Mark W.; Thom, Murray C.; Macready, William G.; Pudenz, Kristen L. (2012). "A Near-Term Quantum Computing Approach for Hard Computational Problems in Space Exploration". arXiv:1204.2821 (https://arxiv.org/abs/1204.2821) [quant-ph (https://arxiv.org/archive/quant-ph)].
27. Boixo, S.; Rønnow, T. F.; Isakov, S. V.; Wang, Z.; Wecker, D.; Lidar, D. A.; Martinis, J. M.; Troyer, M. (2014). "Evidence for quantum annealing with more than one hundred qubits" (http://www.nature.com/nphys/journal/v10/n3/full/nphys2900.html). *Nature Physics*. **10** (3): 218–224. arXiv:1304.4595 (https://arxiv.org/abs/1304.4595). Bibcode:2014NatPh..10..218B (https://ui.adsabs.harvard.edu/abs/2014NatPh..10..218B). doi:10.1038/nphys2900 (https://doi.org/10.1038%2Fnphys2900). S2CID 8031023 (https://api.semanticscholar.org/CorpusID:8031023).
28. "D-Wave Systems Building Quantum Application Ecosystem, Announces Partnerships with DNA-SEQ Alliance and 1QBit" (https://web.archive.org/web/20191231185125/http://www.dwavesys.com/press-releases/d-wave-systems-building-quantum-application-ecosystem-announces-partnerships-dna-seq). *D-Wave Systems*. Archived from the original (http://dwavesys.com/press-releases/d-wave-systems-building-quantum-application-ecosystem-announces-partnerships-dna-seq) on 31 December 2019. Retrieved 22 June 2014.
29. "1QBit Research" (https://web.archive.org/web/20140619053448/http://www.1qbit.com/research.html). *1QBit*. Archived from the original (http://1qbit.com/research.html) on 19 June 2014. Retrieved 22 June 2014.
30. Lanting, T.; Przybysz, A. J.; Smirnov, A. Yu.; Spedalieri, F. M.; et al. (2014-05-29). "Entanglement in a quantum annealing processor". *Physical Review X*. **4** (2): 021041. arXiv:1401.3500 (https://arxiv.org/abs/1401.3500). Bibcode:2014PhRvX...4b1041L (https://ui.adsabs.harvard.edu/abs/2014PhRvX...4b1041L). doi:10.1103/PhysRevX.4.021041 (https://doi.org/10.1103%2FPhysRevX.4.021041). S2CID 19235104 (https://api.semanticscholar.org/CorpusID:19235104).
31. Helmut Katzgraber, quoted in (Cho 2014).
32. Cho, Adrian (20 June 2014). "Quantum or not, controversial computer yields no speedup" (https://doi.org/10.1126%2Fscience.344.6190.1330). *Science*. **344** (6190): 1330–1331. Bibcode:2014Sci...344.1330C (https://ui.adsabs.harvard.edu/abs/2014Sci...344.1330C). doi:10.1126/science.344.6190.1330 (https://doi.org/10.1126%2Fscience.344.6190.1330). PMID 24948715 (https://pubmed.ncbi.nlm.nih.gov/24948715).

33. Amin, Mohammad H. (2015). "Searching for quantum speedup in quasistatic quantum annealers". *Physical Review A*. **92** (5): 052323. arXiv:1503.04216 (https://arxiv.org/abs/1503.04216). Bibcode:2015PhRvA..92e2323A (https://ui.adsabs.harvard.edu/abs/2015PhRvA..92e2323A). doi:10.1103/PhysRevA.92.052323 (https://doi.org/10.1103%2FPhysRevA.92.052323). S2CID 66770023 (https://api.semanticscholar.org/CorpusID:66770023).
34. Steiger, Damian; Heim, Bettina; Rønnow, Troels; Troyer, Matthias (October 22, 2015). "Performance of quantum annealing hardware". In Huckridge, David A.; Ebert, Reinhard; Gruneisen, Mark T.; Dusek, Miloslav; Rarity, John G. (eds.). *Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology*. Vol. 9648. p. 964816. Bibcode:2015SPIE.9648E..16S (https://ui.adsabs.harvard.edu/abs/2015SPIE.9648E..16S). doi:10.1117/12.2202661 (https://doi.org/10.1117%2F12.2202661). S2CID 57916974 (https://api.semanticscholar.org/CorpusID:57916974).
35. "When can Quantum Annealing win?" (http://googleresearch.blogspot.com/2015/12/when-can-quantum-annealing-win.html). *Research Blog*. 8 December 2015. Retrieved 2016-01-21.
36. D-Wave Systems (2021-10-05). "D-Wave's Next-Generation Roadmap: Bringing Clarity to Practical Quantum Computing" (https://dwave.medium.com/d-waves-next-generation-roadmap-bringing-clarity-to-practical-quantum-computing-192b3275c73d). *Medium*. Retrieved 2021-11-12.
37. Venegas-Andraca, Salvador E.; Cruz-Santos, William; McGeoch, Catherine; Lanzagorta, Marco (2018). "A cross-disciplinary introduction to quantum annealing-based algorithms". *Contemporary Physics*. **59** (2): 174–196. arXiv:1803.03372 (https://arxiv.org/abs/1803.03372). Bibcode:2018ConPh..59..174V (https://ui.adsabs.harvard.edu/abs/2018ConPh..59..174V). doi:10.1080/00107514.2018.1450720 (https://doi.org/10.1080%2F00107514.2018.1450720). S2CID 118974781 (https://api.semanticscholar.org/CorpusID:118974781).
38. Ajagekar, Akshay; Humble, Travis; You, Fengqi (2020-01-04). "Quantum computing based hybrid solution strategies for large-scale discrete-continuous optimization problems" (https://doi.org/10.1016%2Fj.compchemeng.2019.106630). *Computers & Chemical Engineering*. **132**: 106630. arXiv:1910.13045 (https://arxiv.org/abs/1910.13045). doi:10.1016/j.compchemeng.2019.106630 (https://doi.org/10.1016%2Fj.compchemeng.2019.106630). ISSN 0098-1354 (https://search.worldcat.org/issn/0098-1354).
39. Wierzbiński, M.; Falo-Roget, J.; Crimi, A. (2023). "Community detection in brain connectomes with hybrid quantum computing" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9977923). *Scientific Reports*. **13** (1): 3446. Bibcode:2023NatSR..13.3446W (https://ui.adsabs.harvard.edu/abs/2023NatSR..13.3446W). doi:10.1038/s41598-023-30579-y (https://doi.org/10.1038%2Fs41598-023-30579-y). PMC 9977923 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9977923). PMID 36859591 (https://pubmed.ncbi.nlm.nih.gov/36859591). S2CID 257236235 (https://api.semanticscholar.org/CorpusID:257236235).

Further reading

- Bapst, V.; Foini, L.; Krzakala, F.; Semerjian, G.; Zamponi, F. (2013). "The quantum adiabatic algorithm applied to random optimization problems: The quantum spin glass perspective". *Physics Reports*. **523** (3): 127–205. arXiv:1210.0811 (https://arxiv.org/abs/1210.0811). Bibcode:2013PhR...523..127B (https://ui.adsabs.harvard.edu/abs/2013PhR...523..127B). doi:10.1016/j.physrep.2012.10.002 (https://doi.org/10.1016%2Fj.physrep.2012.10.002). S2CID 19019744 (https://api.semanticscholar.org/CorpusID:19019744).
- Chandra, Anjan K.; Das, Arnab & Chakrabarti, Bikas K., eds. (2010). *Quantum Quenching, Annealing and Computation*. Lecture Note in Physics. Vol. 802. Heidelberg: Springer. ISBN 978-3-64211-469-4.
- Das, Arnab & Chakrabarti, Bikas K., eds. (2005). *Quantum Annealing and Related Optimization Methods*. Lecture Note in Physics. Vol. 679. Heidelberg: Springer. ISBN 978-3-54027-987-7.

- Dutta, A.; Aeppli, G.; Chakrabarti, B. K.; Divakaran, U.; Rosenbaum, T.F. & Sen, D. (2015). *Quantum Phase Transitions in Transverse Field Spin Models: From Statistical Physics to Quantum Information* (http://www.cambridge.org/us/academic/subjects/physics/quantum-physics-quantum-information-and-quantum-computation/quantum-phase-transitions-transverse-field-spin-models-statistical-physics-quantum-information). Cambridge & Delhi: Cambridge University Press. ISBN 978-1-10706-879-7.
- Li, Fuxiang; Chernyak, V. Y.; Sinitsyn, N. A. (2013). "Quantum Annealing and Computation: A Brief Documentary Note". *Science and Culture*. **79**: 485–500. arXiv:1310.1339 (https://arxiv.org/abs/1310.1339). Bibcode:2013arXiv1310.1339G (https://ui.adsabs.harvard.edu/abs/2013arXiv1310.1339G)..
- Suzuki, S.; Inoue, J.-I. & Chakrabarti, B. K. (2013). "Chapter 8 on Quantum Annealing". *Quantum Ising Phases & Transitions in Transverse Ising Models* (2nd ed.). Heidelberg: Springer. ISBN 978-3-64233-038-4.
- Tanaka, S.; Tamura, R. & Chakrabarti, B. K. (2017). *Quantum Spin Glasses, Annealing & Computation* (http://www.cambridge.org/us/academic/subjects/physics/condensed-matter-physics-nanoscience-and-mesoscopic-physics/quantum-spin-glasses-annealing-and-computation?format=HB#EsrdfXLEbPQs0trI.97). Cambridge & Delhi: Cambridge University Press. ISBN 978-1-10711-319-0.
- "Quantum Annealing & Computation: Challenges & Perspectives" (https://royalsocietypublishing.org/toc/rsta/2023/381/2241). *Philosophical Transactions A*. **381**. Royal Society, London. January 2023.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_annealing&oldid=1231791349"

WIKIPEDIA
The Free Encyclopedia

Quantum counting algorithm

Quantum counting algorithm is a quantum algorithm for efficiently counting the number of solutions for a given search problem. The algorithm is based on the quantum phase estimation algorithm and on Grover's search algorithm.

Counting problems are common in diverse fields such as statistical estimation, statistical physics, networking, etc. As for quantum computing, the ability to perform quantum counting efficiently is needed in order to use Grover's search algorithm (because running Grover's search algorithm requires knowing how many solutions exist). Moreover, this algorithm solves the quantum existence problem (namely, deciding whether *any* solution exists) as a special case.

The algorithm was devised by Gilles Brassard, Peter Høyer and Alain Tapp in 1998.

The problem

Consider a finite set $\{0,1\}^n$ of size $N = 2^n$ and a set B of "solutions" (that is a subset of $\{0,1\}^n$). Define:

$$\begin{cases} f : \{0,1\}^n \to \{0,1\} \\ f(x) = \begin{cases} 1 & x \in B \\ 0 & x \notin B \end{cases} \end{cases}$$

In other words, f is the indicator function of B.

Calculate the number of solutions $M = \left|f^{-1}(1)\right| = |B|$.[1]

Classical solution

Without any prior knowledge on the set of solutions B (or the structure of the function f), a classical deterministic solution cannot perform better than $\Omega(N)$, because all the N elements of $\{0,1\}^n$ must be inspected (consider a case where the last element to be inspected is a solution).

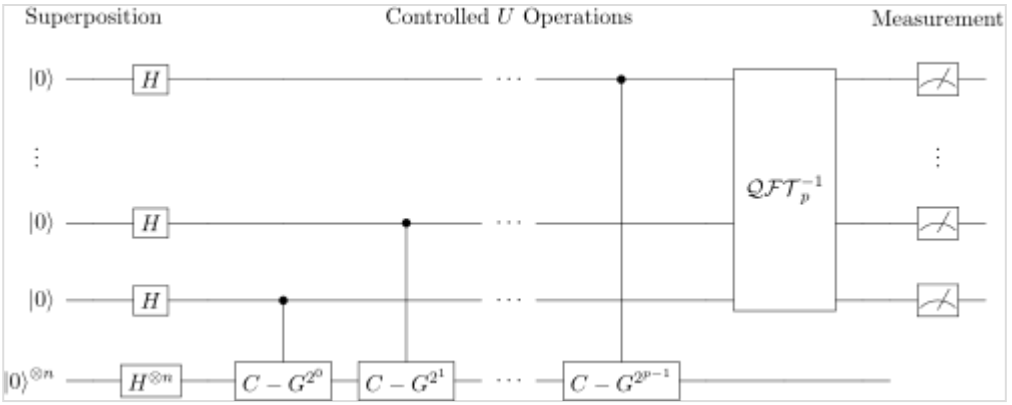
The algorithm

Setup

The input consists of two registers (namely, two parts): the upper p qubits comprise the *first register*, and the lower n qubits are the *second register*.

Create superposition

The initial state of the system is $|0\rangle^{\otimes p}|0\rangle^{\otimes n}$. After applying multiple bit Hadamard gate operation on each of the registers separately, the state of the *first register* is



Quantum counting circuit

$$\frac{1}{2^{p/2}}(|0\rangle + |1\rangle)^{\otimes p}$$

and the state of the *second register* is

$$\frac{1}{2^{n/2}}(|0\rangle + |1\rangle)^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

an equal superposition state in the computational basis.

Grover operator

Because the size of the space is $|\{0,1\}^n| = 2^n = N$ and the number of solutions is $|B| = M$, we can define the normalized states:[2]:252

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_{x\notin B}|x\rangle, \qquad \text{and} \qquad |\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x\in B}|x\rangle.$$

Note that

$$\sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle,$$

which is the state of the *second register* after the Hadamard transform.

Geometric visualization of Grover's algorithm shows that in the two-dimensional space spanned by $|\alpha\rangle$ and $|\beta\rangle$, the Grover operator is a counterclockwise rotation; hence, it can be expressed as

$$G = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

in the orthonormal basis $\{|\alpha\rangle, |\beta\rangle\}$.[2]:252[3]:149

From the properties of rotation matrices we know that G is a unitary matrix with the two eigenvalues $e^{\pm i\theta}$.[2]:253

Estimating the value of θ

From here onwards, we follow the quantum phase estimation algorithm scheme: we apply controlled Grover operations followed by inverse quantum Fourier transform; and according to the analysis, we will find the best p-bit approximation to the real number θ (belonging to the eigenvalues $e^{\pm i\theta}$ of the Grover operator) with probability higher than $\frac{4}{\pi^2}$.[4]:348[3]:157

Note that the second register is actually in a superposition of the eigenvectors of the Grover operator (while in the original quantum phase estimation algorithm, the second register is the required eigenvector). This means that with some probability, we approximate θ, and with some probability, we approximate $2\pi - \theta$; those two approximations are equivalent.[2]:224–225

Analysis

Assuming that the size N of the space is at least twice the number of solutions (namely, assuming that $M \leq \frac{N}{2}$), a result of the analysis of Grover's algorithm is:[2]:254

$$\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}.$$

Thus, if we find θ, we can also find the value of M (because N is known).

The error

$$\frac{|\Delta M|}{N} = \left|\sin^2\left(\frac{\theta+\Delta\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right)\right|$$

is determined by the error within estimation of the value of θ. The quantum phase estimation algorithm finds, with high probability, the best p-bit approximation of θ; this means that if p is large enough, we will have $\Delta\theta \approx 0$, hence $|\Delta M| \approx 0$.[2]:263

Uses

Grover's search algorithm for an initially-unknown number of solutions

In Grover's search algorithm, the number of iterations that should be done is $\frac{\pi}{4}\sqrt{\frac{N}{M}}$.[2]:254 [3]:150

Thus, if N is known and M is calculated by the quantum counting algorithm, the number of iterations for Grover's algorithm is easily calculated.

Speeding up NP-complete problems

The quantum counting algorithm can be used to speed up solution to problems which are NP-complete.

An example of an NP-complete problem is the Hamiltonian cycle problem, which is the problem of determining whether a graph $G = (V, E)$ has a Hamiltonian cycle.

A simple solution to the Hamiltonian cycle problem is checking, for each ordering of the vertices of G, whether it is a Hamiltonian cycle or not. Searching through all the possible orderings of the graph's vertices can be done with quantum counting followed by Grover's algorithm, achieving a speedup of the square root, similar to Grover's algorithm.[2]:264 This approach finds a Hamiltonian cycle (if exists); for determining whether a Hamiltonian cycle exists, the quantum counting algorithm itself is sufficient (and even the quantum existence algorithm, described below, is sufficient).

Quantum existence problem

Quantum existence problem is a special case of quantum counting where we do not want to calculate the value of M, but we only wish to know whether $M \neq 0$ or not.[5]:147

A trivial solution to this problem is directly using the quantum counting algorithm: the algorithm yields M, so by checking whether $M \neq 0$ we get the answer to the existence problem. This approach involves some overhead information because we are not interested in the value of M. Quantum phase estimation can be optimized to eliminate this overhead.[5]:148

If you are not interested in the control of error probability then using a setup with small number of qubits in the upper register will not produce an accurate estimation of the value of θ, but will suffice to determine whether M equals zero or not.[2]:263

Quantum relation testing problem

Quantum relation testing $QRT(value, relation)$. is an extension of quantum existence testing, it decides whether at least one entry can be found in the data base which fulfils the relation to a certain reference value. [6] E.g. $QRT(5, >)$ gives back YES if the data base contains any value larger than 5 else it returns NO. Quantum relation testing combined with classical logarithmic search forms an efficient quantum min/max searching algorithm. [5]:152 [7]

See also

- Quantum phase estimation algorithm
- Grover's algorithm

- Counting problem (complexity)

References

1. Brassard, Gilles; Hoyer, Peter; Tapp, Alain (July 13–17, 1998). *Automata, Languages and Programming* (25th International Colloquium ed.). ICALP'98 Aalborg, Denmark: Springer Berlin Heidelberg. pp. 820–831. arXiv:quant-ph/9805082 (https://arxiv.org/abs/quant-ph/9805082). doi:10.1007/BFb0055105 (https://doi.org/10.1007%2FBFb0055105). ISBN 978-3-540-64781-2. S2CID 14147978 (https://api.semanticscholar.org/CorpusID:14147978).
2. Chuang, Michael A. Nielsen & Isaac L. (2001). *Quantum computation and quantum information* (Repr. ed.). Cambridge [u.a.]: Cambridge Univ. Press. ISBN 978-0521635035.
3. Benenti, Guiliano; Strini, Giulio Casati, Giuliano (2004). *Principles of quantum computation and information* (Reprinted. ed.). New Jersey [u.a.]: World Scientific. ISBN 978-9812388582.
4. Cleve, R.; Ekert, A.; Macchiavello, C.; Mosca, M. (8 January 1998). "Quantum algorithms revisited". *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. **454** (1969): 339–354. arXiv:quant-ph/9708016 (https://arxiv.org/abs/quant-ph/9708016). Bibcode:1998RSPSA.454..339C (https://ui.adsabs.harvard.edu/abs/1998RSPSA.454..339C). doi:10.1098/rspa.1998.0164 (https://doi.org/10.1098%2Frspa.1998.0164). S2CID 16128238 (https://api.semanticscholar.org/CorpusID:16128238).
5. Imre, Sandor; Balazs, Ferenc (January 2005). *Quantum Computing and Communications - An Engineering Approach*. Wiley. ISBN 978-0470869024.
6. Elgaily, Sara; Imre, Sandor (2021). "Constrained Quantum Optimization for Resource Distribution Management". *International Journal of Advanced Computer Science and Applications*. **12** (8).
7. Imre, Sandor (2007). "Quantum Existence Testing and its Application for Finding Extreme Values in Unsorted Databases". *IEEE Transactions on Computers*. **56** (5): 706–710. doi:10.1109/TC.2007.1032 (https://doi.org/10.1109%2FTC.2007.1032). S2CID 29588344 (https://api.semanticscholar.org/CorpusID:29588344).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_counting_algorithm&oldid=1229696821"

WIKIPEDIA
The Free Encyclopedia

Quantum Fourier transform

In quantum computing, the **quantum Fourier transform (QFT)** is a linear transformation on quantum bits, and is the quantum analogue of the discrete Fourier transform. The quantum Fourier transform is a part of many quantum algorithms, notably Shor's algorithm for factoring and computing the discrete logarithm, the quantum phase estimation algorithm for estimating the eigenvalues of a unitary operator, and algorithms for the hidden subgroup problem. The quantum Fourier transform was discovered by Don Coppersmith.[1] With small modifications to the QFT, it can also be used for performing fast integer arithmetic operations such as addition and multiplication.[2][3][4]

The quantum Fourier transform can be performed efficiently on a quantum computer with a decomposition into the product of simpler unitary matrices. The discrete Fourier transform on 2^n amplitudes can be implemented as a quantum circuit consisting of only $O(n^2)$ Hadamard gates and controlled phase shift gates, where n is the number of qubits.[5] This can be compared with the classical discrete Fourier transform, which takes $O(n2^n)$ gates (where n is the number of bits), which is exponentially more than $O(n^2)$.

The quantum Fourier transform acts on a quantum state vector (a quantum register), and the classical Discrete Fourier transform acts on a vector. Both types of vectors can be written as lists of complex numbers. In the classical case, the vector can be represented with e.g. an array of floating point numbers, and in the quantum case it is a sequence of probability amplitudes for all the possible outcomes upon measurement (the outcomes are the *basis states*, or *eigenstates*). Because measurement collapses the quantum state to a single basis state, not every task that uses the classical Fourier transform can take advantage of the quantum Fourier transform's exponential speedup.

The best quantum Fourier transform algorithms known (as of late 2000) require only $O(n \log n)$ gates to achieve an efficient approximation, provided that a controlled phase gate is implemented as a native operation.[6]

Definition

The quantum Fourier transform is the classical discrete Fourier transform applied to the vector of amplitudes of a quantum state, which has length $N = 2^n$ if it is applied to a register of n qubits.

The **classical Fourier transform** acts on a vector $(x_0, x_1, \ldots, x_{N-1}) \in \mathbb{C}^N$ and maps it to the vector $(y_0, y_1, \ldots, y_{N-1}) \in \mathbb{C}^N$ according to the formula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{-nk}, \quad k = 0, 1, 2, \ldots, N-1,$$

where $\omega_N = e^{\frac{2\pi i}{N}}$ is an N-th root of unity.

Similarly, the **quantum Fourier transform** acts on a quantum state $|x\rangle = \sum_{i=0}^{N-1} x_i |i\rangle$ and maps it to a quantum state $\sum_{i=0}^{N-1} y_i |i\rangle$ according to the formula:

$$y_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x_n \omega_N^{nk}, \quad k = 0, 1, 2, \ldots, N-1,$$

(Conventions for the sign of the phase factor exponent vary; here the quantum Fourier transform has the same effect as the inverse discrete Fourier transform, and vice versa.)

Since ω_N^n is a rotation, the **inverse quantum Fourier transform** acts similarly but with:

$$x_n = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k \omega_N^{-nk}, \quad n = 0, 1, 2, \ldots, N-1,$$

In case that $|x\rangle$ is a basis state, the quantum Fourier Transform can also be expressed as the map

$$\mathbf{QFT} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{xk} |k\rangle.$$

Equivalently, the quantum Fourier transform can be viewed as a unitary matrix (or quantum gate) acting on quantum state vectors, where the unitary matrix F_N is the DFT matrix

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

where $\omega = \omega_N$. For example, in the case of $N = 4 = 2^2$ and phase $\omega = i$ the transformation matrix is

$$F_4 = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

Properties

Unitarity

Most of the properties of the quantum Fourier transform follow from the fact that it is a unitary transformation. This can be checked by performing matrix multiplication and ensuring that the relation $FF^\dagger = F^\dagger F = I$ holds, where $F^\dagger$ is the Hermitian adjoint of F. Alternately, one can check that orthogonal vectors of norm 1 get mapped to orthogonal vectors of norm 1.

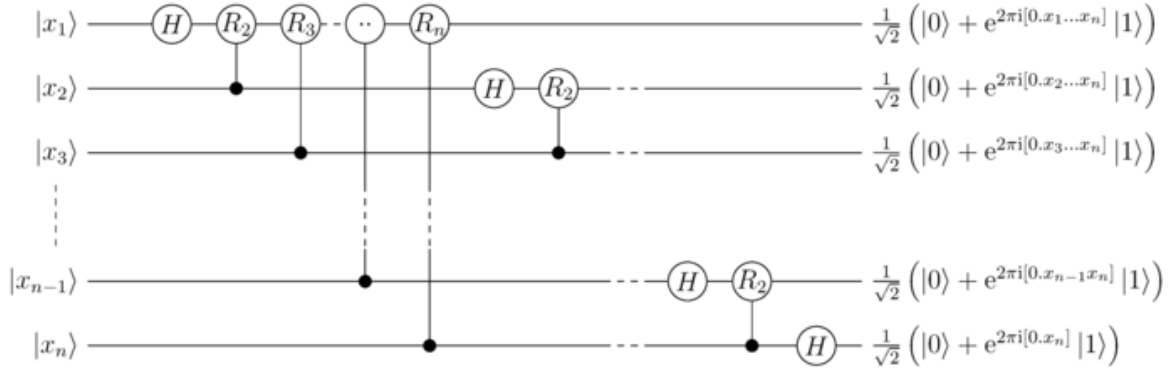
From the unitary property it follows that the inverse of the quantum Fourier transform is the Hermitian adjoint of the Fourier matrix, thus $F^{-1} = F^\dagger$. Since there is an efficient quantum circuit implementing the quantum Fourier transform, the circuit can be run in reverse to perform the inverse quantum Fourier transform. Thus both transforms can be efficiently performed on a quantum computer.

Circuit implementation

The quantum gates used in the circuit of n qubits are the Hadamard gate and the phase gate R_k:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{and} \qquad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i2\pi/2^k} \end{pmatrix}$$

The circuit is composed of H gates and the controlled version of R_k:



An orthonormal basis consists of the basis states

$$|0\rangle, \ldots, |2^n - 1\rangle.$$

These basis states span all possible states of the qubits:

$$|x\rangle = |x_1 x_2 \ldots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$$

where, with tensor product notation $\otimes$, $|x_j\rangle$ indicates that qubit j is in state x_j, with x_j either 0 or 1. By convention, the basis state index x is the binary number encoded by the x_j, with x_1 the most significant bit.

The action of the Hadamard gate is $H|x_i\rangle = \left(\frac{1}{\sqrt{2}}\right)\left(|0\rangle + e^{2\pi i x_i 2^{-1}}|1\rangle\right)$, where the sign depends on x_i.

The quantum Fourier transform can be written as the tensor product of a series of terms:

$$\mathrm{QFT}(|x\rangle) = \frac{1}{\sqrt{N}} \bigotimes_{j=1}^{n} \left(|0\rangle + \omega_N^{x 2^{n-j}}|1\rangle\right).$$

Using the fractional binary notation

$$[0.x_1 \ldots x_m] = \sum_{k=1}^{m} x_k 2^{-k}.$$

the action of the quantum Fourier transform can be expressed in a compact manner:

$$\mathrm{QFT}(|x_1 x_2 \ldots x_n\rangle) = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i\,[0.x_n]}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i\,[0.x_{n-1}x_n]}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i\,[0.x_1 x_2 \ldots x_n]}|1\rangle\right).$$

To obtain this state from the circuit depicted above, a swap operation of the qubits must be performed to reverse their order. At most $n/2$ swaps are required.[5]

Because the discrete Fourier transform, an operation on *n* qubits, can be factored into the tensor product of *n* single-qubit operations, it is easily represented as a quantum circuit (up to an order reversal of the output). Each of those single-qubit operations can be implemented efficiently using one Hadamard gate and a linear number of controlled phase gates. The first term requires one Hadamard gate and $(n-1)$ controlled phase gates, the next term requires one Hadamard gate and $(n-2)$ controlled phase gate, and each following term requires one fewer controlled phase gate. Summing up the number of gates, excluding the ones needed for the output reversal, gives $n + (n-1) + \cdots + 1 = n(n+1)/2 = O(n^2)$ gates, which is quadratic polynomial in the number of qubits. This value is much smaller than for the classical Fourier transformation.[7]

The circuit-level implementation of the quantum Fourier transform on a linear nearest neighbor architecture has been studied before.[8][9] The circuit depth is linear in the number of qubits.

Example

The quantum Fourier transform on three qubits, F_8 with $n = 3, N = 8 = 2^3$, is represented by the following transformation:

$$\mathbf{QFT} : |x\rangle \mapsto \frac{1}{\sqrt{8}} \sum_{k=0}^{7} \omega^{xk} |k\rangle,$$

where $\omega = \omega_8$ is an eighth root of unity satisfying $\omega^8 = \left(e^{\frac{i2\pi}{8}}\right)^8 = 1$.

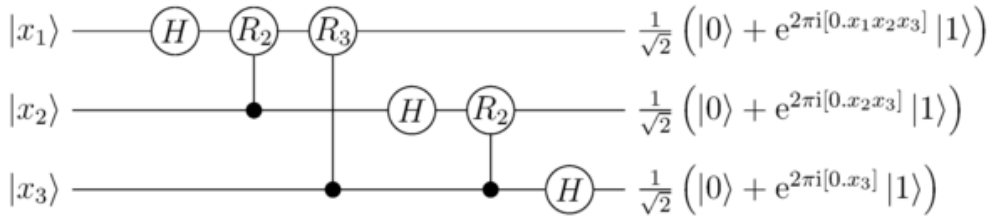
The matrix representation of the Fourier transform on three qubits is:

$$F_8 = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}.$$

The 3-qubit quantum Fourier transform can be rewritten as:

$$\mathbf{QFT}(|x_1, x_2, x_3\rangle) = \frac{1}{\sqrt{8}} \left(|0\rangle + e^{2\pi i\,[0.x_3]}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i\,[0.x_2 x_3]}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i\,[0.x_1 x_2 x_3]}|1\rangle\right).$$

The following sketch shows the respective circuit for $n = 3$ (with reversed order of output qubits with respect to the proper QFT):



As calculated above, the number of gates used is $n(n+1)/2$ which is equal to 6, for $n = 3$.

Relation to quantum Hadamard transform

Using the generalized Fourier transform on finite (abelian) groups, there are actually two natural ways to define a quantum Fourier transform on an *n*-qubit quantum register. The QFT as defined above is equivalent to the DFT, which considers these n qubits as indexed by the cyclic group $\mathbb{Z}/2^n\mathbb{Z}$. However, it also makes sense to consider the qubits as indexed by the Boolean group $(\mathbb{Z}/2\mathbb{Z})^n$, and in this case the Fourier transform is the Hadamard transform. This is achieved by applying a Hadamard gate to each of the n qubits in parallel.[10][11] Shor's algorithm uses both types of Fourier transforms, an initial Hadamard transform as well as a QFT.

For other groups

The Fourier transform can be formulated for groups other than the cyclic group, and extended to the quantum setting.[12] For example, consider the symmetric group S_n.[13][14] The Fourier transform can be expressed in matrix form

$$\mathfrak{F}_n = \sum_{\lambda \in \Lambda_n} \sum_{p,q \in \mathcal{P}(\lambda)} \sum_{g \in S_n} \sqrt{\frac{d_\lambda}{n!}} [\lambda(g)]_{q,p} |\lambda, p, q\rangle\langle g|$$

where $[\lambda(g)]_{q,p}$ is the (q,p) element of the matrix representation of $\lambda(g)$, $\mathcal{P}(\lambda)$ is the set of paths from the root node to λ in the Bratteli diagram of S_n, Λ_n is the set of representations of S_n indexed by Young diagrams, and g is a permutation.

Over a finite field

The discrete Fourier transform can also be formulated over a finite field F_q, and a quantum version can be defined.[15] Here $N = q = p^n$. Let $\phi : GF(q) \to GF(p)$ be an arbitrary linear map (trace, for example). Then for each $x \in GF(q)$ define

$$F_{q,\phi} : |x\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{y \in GF(q)} \omega^{\phi(xy)} |y\rangle$$

for $\omega = e^{2\pi i/p}$ and extend $F_{q,\phi}$ linearly.

References

1. Coppersmith, D. (2002). An approximate Fourier transform useful in quantum factoring (Preprint). arXiv:quant-ph/0201067 (https://arxiv.org/abs/quant-ph/0201067).
2. Draper, Thomas G. (7 Aug 2000). "Addition on a Quantum Computer". arXiv:quant-ph/0008033 (https://arxiv.org/abs/quant-ph/0008033).
3. Ruiz-Perez, Lidia; Juan Carlos, Garcia-Escartin (2 May 2017). "Quantum arithmetic with the quantum Fourier transform". *Quantum Information Processing*. **16** (6): 152. arXiv:1411.5949v2 (https://arxiv.org/abs/1411.5949v2). Bibcode:2017QuIP...16..152R (https://ui.adsabs.harvard.edu/abs/2017QuIP...16..152R). doi:10.1007/s11128-017-1603-1 (https://doi.org/10.1007%2Fs11128-017-1603-1). S2CID 10948948 (https://api.semanticscholar.org/CorpusID:10948948).
4. Şahin, Engin (2020). "Quantum arithmetic operations based on quantum Fourier transform on signed integers". *International Journal of Quantum Information*. **18** (6): 2050035. arXiv:2005.00443v3 (https://arxiv.org/abs/2005.00443v3). doi:10.1142/s0219749920500355 (https://doi.org/10.1142%2Fs0219749920500355). ISSN 1793-6918 (https://search.worldcat.org/issn/1793-6918).
5. Nielsen, Michael A.; Chuang, Isaac L. (2012). *Quantum Computation and Quantum Information*. doi:10.1017/CBO9780511976667 (https://doi.org/10.1017%2FCBO9780511976667). ISBN 978-1-107-00217-3.
6. Hales, L.; Hallgren, S. (November 12–14, 2000). "An improved quantum Fourier transform algorithm and applications". *Proceedings 41st Annual Symposium on Foundations of Computer Science*. pp. 515–525. CiteSeerX 10.1.1.29.4161 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.29.4161). doi:10.1109/SFCS.2000.892139 (https://doi.org/10.1109%2FSFCS.2000.892139). ISBN 0-7695-0850-2. S2CID 424297 (https://api.semanticscholar.org/CorpusID:424297).
7. Kurgalin, Sergei; Borzunov, Sergei (2021). *Concise guide to quantum computing: algorithms, exercises, and implementations*. Texts in computer science. Cham: Springer. ISBN 978-3-030-65054-4.
8. Fowler, A.G.; Devitt, S.J.; Hollenberg, L.C.L. (July 2004). "Implementation of Shor's algorithm on a linear nearest neighbour qubit array". *Quantum Information and Computation*. **4** (4): 237–251. doi:10.26421/QIC4.4-1 (https://doi.org/10.26421%2FQIC4.4-1).
9. Maslov, Dmitri (15 November 2007). "Linear depth stabilizer and quantum Fourier transformation circuits with no auxiliary qubits in finite-neighbor quantum architectures". *Physical Review A*. **76** (5): 052310. arXiv:quant-ph/0703211 (https://arxiv.org/abs/quant-ph/0703211). Bibcode:2007PhRvA..76e2310M (https://ui.adsabs.harvard.edu/abs/2007PhRvA..76e2310M). doi:10.1103/PhysRevA.76.052310 (https://doi.org/10.1103%2FPhysRevA.76.052310). S2CID 18645435 (https://api.semanticscholar.org/CorpusID:18645435).
10. Fourier Analysis of Boolean Maps– A Tutorial –, pp. 12-13 (https://www.staff.uni-mainz.de/pommeren/Kryptologie/Bitblock/A_Nonlin/Fourier.pdf)
11. Lecture 5: Basic quantum algorithms, Rajat Mittal, pp. 4-5 (https://www.cse.iitk.ac.in/users/rmittal/prev_course/s19/reports/5_algo.pdf)
12. Moore, Cristopher; Rockmore, Daniel; Russell, Alexander (2003). Generic Quantum Fourier Transforms (Preprint). arXiv:quant-ph/0304064 (https://arxiv.org/abs/quant-ph/0304064).
13. Kawano, Yasuhito; Sekigawa, Hiroshi (July 2016). "Quantum Fourier transform over symmetric groups — improved result". *Journal of Symbolic Computation*. **75**: 219–243. doi:10.1016/j.jsc.2015.11.016 (https://doi.org/10.1016%2Fj.jsc.2015.11.016).
14. Beals, Robert (1997). "Quantum computation of Fourier transforms over symmetric groups". *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing - STOC '97*. pp. 48–53. doi:10.1145/258533.258548 (https://doi.org/10.1145%2F258533.258548). ISBN 0-89791-888-6.

15. de Beaudrap, Niel; Cleve, Richard; Waltrous, John (8 November 2002). "Sharp Quantum versus Classical Query Complexity Separations". *Algorithmica*. **34** (4): 449–461. doi:10.1007/s00453-002-0978-1 (https://doi.org/10.1007%2Fs00453-002-0978-1).

Further reading

- Parthasarathy, K. R. (2006). *Lectures on Quantum Computation, Quantum Error Correcting Codes and Information Theory*. Tata Institute of Fundamental Research. ISBN 978-81-7319-688-1.
- Preskill, John (September 1998). "Lecture Notes for Physics 229: Quantum Information and Computation" (https://web.gps.caltech.edu/~rls/book.pdf) (PDF).

External links

- Wolfram Demonstration Project: Quantum Circuit Implementing Grover's Search Algorithm (http://demonstrations.wolfram.com/QuantumCircuitImplementingGroversSearchAlgorithm/)
- Wolfram Demonstration Project: Quantum Circuit Implementing Quantum Fourier Transform (http://demonstrations.wolfram.com/QuantumFourierTransformCircuit/)
- Quirk online life quantum fourier transform (http://algassert.com/quirk#circuit=%7B%22cols%22%3A%5B%5B%22Counting8%22%5D%2C%5B%22Chance8%22%5D%2C%5B%22%E2%80%A6%22%2C%22%E2%80%A6%22%2C%22%E2%80%A6%22%2C%22%E2%80%A6%22%2C%22%E2%80%A6%22%2C%22%E2%80%A6%22%2C%22%E2%80%A6%22%5D%2C%5B%22Swap%22%2C1%2C1%2C1%2C1%2C1%2C1%2C%22Swap%22%5D%2C%5B1%2C%22Swap%22%2C1%2C1%2C1%2C1%2C%22Swap%22%5D%2C%5B1%2C1%2C%22Swap%22%2C1%2C1%2C%22Swap%22%5D%2C%5B1%2C1%2C1%2C%22Swap%22%2C%22Swap%22%5D%2C%5B%22H%22%5D%2C%5B%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C%22H%22%5D%2C%5B%22Z%5E%C2%BC%22%2C%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C1%2C%22H%22%5D%2C%5B%22Z%5E%E2%85%9B%22%2C%22Z%5E%C2%BC%22%2C%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C1%2C1%2C%22H%22%5D%2C%5B%22Z%5E%E2%85%9F%E2%82%81%E2%82%86%22%2C%22Z%5E%E2%85%9B%22%2C%22Z%5E%C2%BC%22%2C%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C1%2C1%2C1%2C%22H%22%5D%2C%5B%22Z%5E%E2%85%9F%E2%82%83%E2%82%82%22%2C%22Z%5E%E2%85%9F%E2%82%81%E2%82%86%22%2C%22Z%5E%E2%85%9B%22%2C%22Z%5E%C2%BC%22%2C%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C1%2C1%2C1%2C1%2C%22H%22%5D%2C%5B%22Z%5E%E2%85%9F%E2%82%86%E2%82%84%22%2C%22Z%5E%E2%85%9F%E2%82%83%E2%82%82%22%2C%22Z%5E%E2%85%9F%E2%82%81%E2%82%86%22%2C%22Z%5E%E2%85%9B%22%2C%22Z%5E%C2%BC%22%2C%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C1%2C1%2C1%2C1%2C1%2C%22H%22%5D%2C%5B%22Z%5E%E2%85%9F%E2%82%81%E2%82%82%E2%82%88%22%2C%22Z%5E%E2%85%9F%E2%82%86%E2%82%84%22%2C%22Z%5E%E2%85%9F%E2%82%83%E2%82%82%22%2C%22Z%5E%E2%85%9F%E2%82%81%E2%82%86%22%2C%22Z%5E%E2%85%9B%22%2C%22Z%5E%C2%BC%22%2C%22Z%5E%C2%BD%22%2C%22%E2%80%A2%22%5D%2C%5B1%2C1%2C1%2C1%2C1%2C1%2C1%2C%22H%22%5D%5D%7D)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_Fourier_transform&oldid=1245324632"

WIKIPEDIA
The Free Encyclopedia

Quantum optimization algorithms

Quantum optimization algorithms are quantum algorithms that are used to solve optimization problems.[1] Mathematical optimization deals with finding the best solution to a problem (according to some criteria) from a set of possible solutions. Mostly, the optimization problem is formulated as a minimization problem, where one tries to minimize an error which depends on the solution: the optimal solution has the minimal error. Different optimization techniques are applied in various fields such as mechanics, economics and engineering, and as the complexity and amount of data involved rise, more efficient ways of solving optimization problems are needed. Quantum computing may allow problems which are not practically feasible on classical computers to be solved, or suggest a considerable speed up with respect to the best known classical algorithm.

Quantum data fitting

Data fitting is a process of constructing a mathematical function that best fits a set of data points. The fit's quality is measured by some criteria, usually the distance between the function and the data points.

Quantum least squares fitting

One of the most common types of data fitting is solving the least squares problem, minimizing the sum of the squares of differences between the data points and the fitted function.

The algorithm is given N input data points $(x_1, y_1), (x_2, y_2), \ldots, (x_N, y_N)$ and M continuous functions $f_1, f_2, \ldots, f_M$. The algorithm finds and gives as output a continuous function $f_{\vec{\lambda}}$ that is a linear combination of f_j:

$$f_{\vec{\lambda}}(x) = \sum_{j=1}^{M} f_j(x)\lambda_j$$

In other words, the algorithm finds the complex coefficients λ_j, and thus the vector $\vec{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_M)$.

The algorithm is aimed at minimizing the error, which is given by:

$$E = \sum_{i=1}^{N} \left| f_{\vec{\lambda}}(x_i) - y_i \right|^2 = \sum_{i=1}^{N} \left| \sum_{j=1}^{M} f_j(x_i)\lambda_j - y_i \right|^2 = \left| F\vec{\lambda} - \vec{y} \right|^2$$

where F is defined to be the following matrix:

$$F = \begin{pmatrix} f_1(x_1) & \cdots & f_M(x_1) \\ f_1(x_2) & \cdots & f_M(x_2) \\ \vdots & \ddots & \vdots \\ f_1(x_N) & \cdots & f_M(x_N) \end{pmatrix}$$

The quantum least-squares fitting algorithm[2] makes use of a version of Harrow, Hassidim, and Lloyd's quantum algorithm for linear systems of equations (HHL), and outputs the coefficients λ_j and the fit quality estimation E. It consists of three subroutines: an algorithm for performing a pseudo-inverse operation, one routine for the fit quality estimation, and an algorithm for learning the fit parameters.

Because the quantum algorithm is mainly based on the HHL algorithm, it suggests an exponential improvement[3] in the case where F is sparse and the condition number (namely, the ratio between the largest and the smallest eigenvalues) of both $FF^\dagger$ and $F^\dagger F$ is small.

Quantum semidefinite programming

Semidefinite programming (SDP) is an optimization subfield dealing with the optimization of a linear objective function (a user-specified function to be minimized or maximized), over the intersection of the cone of positive semidefinite matrices with an affine space. The objective function is an inner product of a matrix C (given as an input) with the variable X. Denote by $\mathbb{S}^n$ the space of all $n \times n$ symmetric matrices. The variable X must lie in the (closed convex) cone of positive semidefinite symmetric matrices $\mathbb{S}^n_+$. The inner product of two matrices is defined as:

$$\langle A, B \rangle_{\mathbb{S}^n} = \mathrm{tr}(A^T B) = \sum_{i=1,j=1}^{n} A_{ij} B_{ij}.$$

The problem may have additional constraints (given as inputs), also usually formulated as inner products. Each constraint forces the inner product of the matrices A_k (given as an input) with the optimization variable X to be smaller than a specified value b_k (given as an input). Finally, the SDP problem can be written as:

$$\begin{aligned} \min_{X \in \mathbb{S}^n} \quad & \langle C, X \rangle_{\mathbb{S}^n} \\ \text{subject to} \quad & \langle A_k, X \rangle_{\mathbb{S}^n} \leq b_k, \quad k = 1, \ldots, m \\ & X \succeq 0 \end{aligned}$$

The best classical algorithm is not known to unconditionally run in polynomial time. The corresponding feasibility problem is known to either lie outside of the union of the complexity classes NP and co-NP, or in the intersection of NP and co-NP.[4]

The quantum algorithm

The algorithm inputs are $A_1 \ldots A_m, C, b_1 \ldots b_m$ and parameters regarding the solution's trace, precision and optimal value (the objective function's value at the optimal point).

The quantum algorithm[5] consists of several iterations. In each iteration, it solves a feasibility problem, namely, finds any solution satisfying the following conditions (giving a threshold t):

$$\begin{aligned}
&\langle C, X\rangle_{\mathbb{S}^n} \leq t \\
&\langle A_k, X\rangle_{\mathbb{S}^n} \leq b_k, \quad k = 1, \ldots, m \\
&X \succeq 0
\end{aligned}$$

In each iteration, a different threshold t is chosen, and the algorithm outputs either a solution X such that $\langle C, X\rangle_{\mathbb{S}^n} \leq t$ (and the other constraints are satisfied, too) or an indication that no such solution exists. The algorithm performs a binary search to find the minimal threshold t for which a solution X still exists: this gives the minimal solution to the SDP problem.

The quantum algorithm provides a quadratic improvement over the best classical algorithm in the general case, and an exponential improvement when the input matrices are of low rank.

Quantum combinatorial optimization

The combinatorial optimization problem is aimed at finding an optimal object from a finite set of objects. The problem can be phrased as a maximization of an objective function which is a sum of boolean functions. Each boolean function $C_\alpha : \{0,1\}^n \to \{0,1\}$ gets as input the n-bit string $z = z_1 z_2 \ldots z_n$ and gives as output one bit (0 or 1). The combinatorial optimization problem of n bits and m clauses is finding an n-bit string z that maximizes the function

$$C(z) = \sum_{\alpha=1}^{m} C_\alpha(z)$$

Approximate optimization is a way of finding an approximate solution to an optimization problem, which is often NP-hard. The approximated solution of the combinatorial optimization problem is a string z that is close to maximizing $C(z)$.

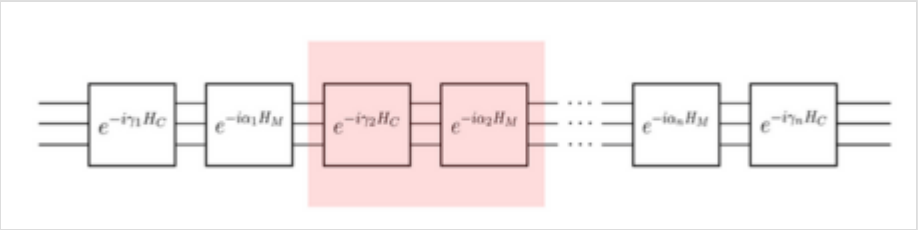
Quantum approximate optimization algorithm

For combinatorial optimization, the **quantum approximate optimization algorithm** (QAOA)[6] briefly had a better approximation ratio than any known polynomial time classical algorithm (for a certain problem),[7] until a more effective classical algorithm was proposed.[8] The relative speed-up of the quantum algorithm is an open research question.

QAOA consists of the following steps:

1. Defining a *cost Hamiltonian* H_C such that its ground state encodes the solution to the optimization problem.
2. Defining a *mixer Hamiltonian* H_M.
3. Defining the oracles $U_C(\gamma) = \exp(-i\gamma H_C)$ and $U_M(\alpha) = \exp(-i\alpha H_M)$, with parameters γ and α.

4. Repeated application of the oracles U_C and U_M, in the order:
$$U(\boldsymbol{\gamma}, \boldsymbol{\alpha}) = \prod_{i=1}^{N} (U_C(\gamma_i) U_M(\alpha_i))$$
5. Preparing an initial state, that is a superposition of all possible states and apply $U(\boldsymbol{\gamma}, \boldsymbol{\alpha})$ to the state.
6. Using classical methods to optimize the parameters $\boldsymbol{\gamma}, \boldsymbol{\alpha}$ and measure the output state of the optimized circuit to obtain the approximate optimal solution to the cost Hamiltonian. An optimal solution will be one that maximizes the expectation value of the cost Hamiltonian H_C.



Sample QAOA ansatz for a three qubit circuit

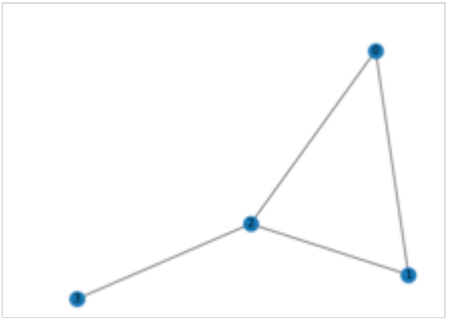
The layout of the algorithm, viz, the use of cost and mixer Hamiltonians are inspired from the Quantum Adiabatic theorem, which states that starting in a ground state of a time-dependent Hamiltonian, if the Hamiltonian evolves slowly enough, the final state will be a ground state of the final Hamiltonian. Moreover, the adiabatic theorem can be generalized to any other eigenstate as long as there is no overlap (degeneracy) between different eigenstates across the evolution. Identifying the initial Hamiltonian with H_M and the final Hamiltonian with H_C, whose ground states encode the solution to the optimization problem of interest, one can approximate the optimization problem as the adiabatic evolution of the Hamiltonian from an initial to the final one, whose ground (eigen)state gives the optimal solution. In general, QAOA relies on the use of unitary operators dependent on $2p$ angles (parameters), where $p > 1$ is an input integer, which can be identified the number of layers of the oracle $U(\boldsymbol{\gamma}, \boldsymbol{\alpha})$. These operators are iteratively applied on a state that is an equal-weighted quantum superposition of all the possible states in the computational basis. In each iteration, the state is measured in the computational basis and the boolean function $C(z)$ is estimated. The angles are then updated classically to increase $C(z)$. After this procedure is repeated a sufficient number of times, the value of $C(z)$ is almost optimal, and the state being measured is close to being optimal as well. A sample circuit that implements QAOA on a quantum computer is given in figure. This procedure is highlighted using the following example of finding the minimum vertex cover of a graph.[9]

QAOA for finding the minimum vertex cover of a graph

The goal here is to find a minimum vertex cover of a graph: a collection of vertices such that each edge in the graph contains at least one of the vertices in the cover. Hence, these vertices “cover” all the edges. We wish to find a vertex cover that has the smallest possible number of vertices. Vertex covers can be represented by a bit string where each bit denotes whether the corresponding vertex is present in the cover. For example, the bit string 0101 represents a cover consisting of the second and fourth vertex in a graph with four vertices.

Consider the graph given in the figure. It has four vertices and there are two minimum vertex cover for this graph: vertices 0 and 2, and the vertices 1 and 2. These can be respectively represented by the bit strings 1010 and 0110. The goal of the algorithm is to sample these bit strings with high probability. In

this case, the cost Hamiltonian has two ground states, |1010⟩ and |0110⟩, coinciding with the solutions of the problem. The mixer Hamiltonian is the simple, non-commuting sum of Pauli-X operations on each node of the graph and they are given by:

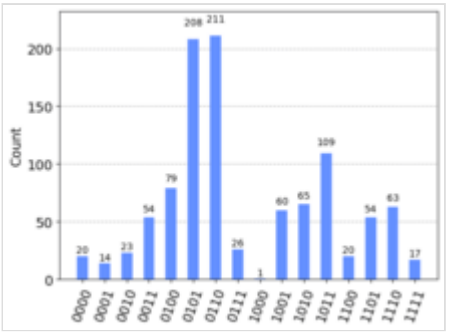


Sample graph to illustrate the minimum vertex cover problem.

$$H_C = -0.25Z_3 + 0.5Z_0 + 0.5Z_1 + 1.25Z_2 + 0.75(Z_0Z_1 + Z_0Z_2 + Z_2Z_3 + Z_1Z_2)$$

$$H_M = X_0 + X_1 + X_2 + X_3$$

Implementing QAOA algorithm for this four qubit circuit with two layers of the ansatz in qiskit (see figure) and optimizing leads to a probability distribution for the states given in the figure. This shows that the states |0110⟩ and |1010⟩ have the highest probabilities of being measured, just as expected.



Output of QAOA implementation in Qiskit for minimum vertex cover problem. Note that the bit string |1010> is flipped as |0101> as Qiskit uses reverse ordering of bits.

Generalization of QAOA to constrained combinatorial optimisation

In principle the optimal value of $C(z)$ can be reached up to arbitrary precision, this is guaranteed by the adiabatic theorem[10][11] or alternatively by the universality of the QAOA unitaries.[12] However, it is an open question whether this can be done in a feasible way. For example, it was shown that QAOA exhibits a strong dependence on the ratio of a problem's constraint to variables (problem density) placing a limiting restriction on the algorithm's capacity to minimize a corresponding objective function.[13]



Qiskit implementation of QAOA for minimum vertex cover problem.

It was soon recognized that a generalization of the QAOA process is essentially an alternating application of a continuous-time quantum walk on an underlying graph followed by a quality-dependent phase shift applied to each solution state. This generalized QAOA was termed as QWOA (Quantum Walk-based Optimisation Algorithm).[14]

In the paper *How many qubits are needed for quantum computational supremacy* submitted to arXiv,[15] the authors conclude that a QAOA circuit with 420 qubits and 500 constraints would require at least one century to be simulated using a classical simulation algorithm running on state-of-the-art supercomputers so that would be sufficient for quantum computational supremacy.

A rigorous comparison of QAOA with classical algorithms can give estimates on depth p and number of qubits required for quantum advantage. A study of QAOA and MaxCut algorithm shows that $p > 11$ is required for scalable advantage.[16]

Variations of QAOA

Several variations to the basic structure of QAOA have been proposed,[17] which include variations to the ansatz of the basic algorithm. The choice of ansatz typically depends on the problem type, such as combinatorial problems represented as graphs, or problems strongly influenced by hardware design. However, ansatz design must balance specificity and generality to avoid overfitting and maintain applicability to a wide range of problems. For this reason, designing optimal ansatze for QAOA is an extensively researched and widely investigated topic. Some of the proposed variants are:

1. Multi-angle QAOA[18]
2. QAOA+[19]
3. Digitised counteradiabatic QAOA[20]
4. Quantum alternating operator ansatz[21],which allows for constrains on the optimization problem etc.

Another variation of QAOA focuses on techniques for parameter optimization, which aims at selecting the optimal set of initial parameters for a given problem and avoiding barren plateaus, which represent parameters leading to eigenstates which correspond to plateaus in the energy landscape of the cost Hamiltonian.

Finally, there has been significant research interest in leveraging specific hardware to enhance the performance of QAOA across various platforms, such as trapped ion, neutral atoms, superconducting qubits, and photonic quantum computers. The goals of these approaches include overcoming hardware connectivity limitations and mitigating noise-related issues to broaden the applicability of QAOA to a wide range of combinatorial optimization problems.

See also

- Adiabatic quantum computation
- Quantum annealing

References

1. Moll, Nikolaj; Barkoutsos, Panagiotis; Bishop, Lev S.; Chow, Jerry M.; Cross, Andrew; Egger, Daniel J.; Filipp, Stefan; Fuhrer, Andreas; Gambetta, Jay M.; Ganzhorn, Marc; Kandala, Abhinav; Mezzacapo, Antonio; Müller, Peter; Riess, Walter; Salis, Gian; Smolin, John; Tavernelli, Ivano; Temme, Kristan (2018). "Quantum optimization using variational algorithms on near-term quantum devices". *Quantum Science and Technology*. **3** (3): 030503. arXiv:1710.01022 (https://arxiv.org/abs/1710.01022). Bibcode:2018QS&T....3c0503M (https://ui.adsabs.harvard.edu/abs/2018QS&T....3c0503M). doi:10.1088/2058-9565/aab822 (https://doi.org/10.1088%2F2058-9565%2Faab822). S2CID 56376912 (https://api.semanticscholar.org/CorpusID:56376912).

2. Wiebe, Nathan; Braun, Daniel; Lloyd, Seth (2 August 2012). "Quantum Algorithm for Data Fitting". *Physical Review Letters*. **109** (5): 050505. arXiv:1204.5242 (https://arxiv.org/abs/1204.5242). Bibcode:2012PhRvL.109e0505W (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109e0505W). doi:10.1103/PhysRevLett.109.050505 (https://doi.org/10.1103%2FPhysRevLett.109.050505). PMID 23006156 (https://pubmed.ncbi.nlm.nih.gov/23006156). S2CID 118439810 (https://api.semanticscholar.org/CorpusID:118439810).
3. Montanaro, Ashley (12 January 2016). "Quantum algorithms: an overview". *npj Quantum Information*. **2**: 15023. arXiv:1511.04206 (https://arxiv.org/abs/1511.04206). Bibcode:2016npjQI...215023M (https://ui.adsabs.harvard.edu/abs/2016npjQI...215023M). doi:10.1038/npjqi.2015.23 (https://doi.org/10.1038%2Fnpjqi.2015.23). S2CID 2992738 (https://api.semanticscholar.org/CorpusID:2992738).
4. Ramana, Motakuri V. (1997). "An exact duality theory for semidefinite programming and its complexity implications" (https://doi.org/10.1007/BF02614433). *Mathematical Programming*. **77**: 129–162. doi:10.1007/BF02614433 (https://doi.org/10.1007%2FBF02614433). S2CID 12886462 (https://api.semanticscholar.org/CorpusID:12886462).
5. Brandao, Fernando G. S. L.; Svore, Krysta (2016). "Quantum Speed-ups for Semidefinite Programming". arXiv:1609.05537 (https://arxiv.org/abs/1609.05537) [quant-ph (https://arxiv.org/archive/quant-ph)].
6. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
7. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014). "A Quantum Approximate Optimization Algorithm Applied to a Bounded Occurrence Constraint Problem". arXiv:1412.6062 (https://arxiv.org/abs/1412.6062) [quant-ph (https://arxiv.org/archive/quant-ph)].
8. Barak, Boaz; Moitra, Ankur; O'Donnell, Ryan; Raghavendra, Prasad; Regev, Oded; Steurer, David; Trevisan, Luca; Vijayaraghavan, Aravindan; Witmer, David; Wright, John (2015). "Beating the random assignment on constraint satisfaction problems of bounded degree". arXiv:1505.03424 (https://arxiv.org/abs/1505.03424) [cs.CC (https://arxiv.org/archive/cs.CC)].
9. Ceroni, Jack (2020-11-18). "Intro to QAOA" (https://pennylane.aiundefined/). *PennyLane Demos*.
10. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
11. Binkowski, Lennart; Koßmann, Gereon; Ziegler, Timo; Schwonnek, René (2024). "Elementary proof of QAOA convergence". *New Journal of Physics*. **26** (7): 073001. arXiv:2302.04968 (https://arxiv.org/abs/2302.04968). doi:10.1088/1367-2630/ad59bb (https://doi.org/10.1088%2F1367-2630%2Fad59bb).
12. Morales, M. E.; Biamonte, J. D.; Zimborás, Z. (2019-09-20). "On the universality of the quantum approximate optimization algorithm". *Quantum Information Processing*. **19** (9): 291. arXiv:1909.03123 (https://arxiv.org/abs/1909.03123). doi:10.1007/s11128-020-02748-9 (https://doi.org/10.1007%2Fs11128-020-02748-9).
13. Akshay, V.; Philathong, H.; Morales, M. E. S.; Biamonte, J. D. (2020-03-05). "Reachability Deficits in Quantum Approximate Optimization". *Physical Review Letters*. **124** (9): 090504. arXiv:1906.11259 (https://arxiv.org/abs/1906.11259). Bibcode:2020PhRvL.124i0504A (https://ui.adsabs.harvard.edu/abs/2020PhRvL.124i0504A). doi:10.1103/PhysRevLett.124.090504 (https://doi.org/10.1103%2FPhysRevLett.124.090504). PMID 32202873 (https://pubmed.ncbi.nlm.nih.gov/32202873). S2CID 195699685 (https://api.semanticscholar.org/CorpusID:195699685).

14. Marsh, S.; Wang, J. B. (2020-06-08). "Combinatorial optimization via highly efficient quantum walks". *Physical Review Research*. **2** (2): 023302. arXiv:1912.07353 (https://arxiv.org/abs/1912.07353). Bibcode:2020PhRvR...2b3302M (https://ui.adsabs.harvard.edu/abs/2020PhRvR...2b3302M). doi:10.1103/PhysRevResearch.2.023302 (https://doi.org/10.1103%2FPhysRevResearch.2.023302). S2CID 216080740 (https://api.semanticscholar.org/CorpusID:216080740).
15. Dalzell, Alexander M.; Harrow, Aram W.; Koh, Dax Enshan; La Placa, Rolando L. (2020-05-11). "How many qubits are needed for quantum computational supremacy?" (https://doi.org/10.22331%2Fq-2020-05-11-264). *Quantum*. **4**: 264. arXiv:1805.05224 (https://arxiv.org/abs/1805.05224). Bibcode:2020Quant...4..264D (https://ui.adsabs.harvard.edu/abs/2020Quant...4..264D). doi:10.22331/q-2020-05-11-264 (https://doi.org/10.22331%2Fq-2020-05-11-264). ISSN 2521-327X (https://search.worldcat.org/issn/2521-327X).
16. Lykov, Danylo; Wurtz, Jonathan; Poole, Cody; Saffman, Mark; Noel, Tom; Alexeev, Yuri (2023). "Sampling frequency thresholds for the quantum advantage of the quantum approximate optimization algorithm". *npj Quantum Information*. **9**: 73. arXiv:2206.03579 (https://arxiv.org/abs/2206.03579). Bibcode:2023npjQI...9...73L (https://ui.adsabs.harvard.edu/abs/2023npjQI...9...73L). doi:10.1038/s41534-023-00718-4 (https://doi.org/10.1038%2Fs41534-023-00718-4).
17. Blekos, Kostas; Brand, Dean; Ceschini, Andrea; Chou, Chiao-Hui; Li, Rui-Hao; Pandya, Komal; Summer, Alessandro (June 2024). "A Review on Quantum Approximate Optimization Algorithm and its Variants". *Physics Reports*. **1068**: 1–66. arXiv:2306.09198 (https://arxiv.org/abs/2306.09198). Bibcode:2024PhR..1068....1B (https://ui.adsabs.harvard.edu/abs/2024PhR..1068....1B). doi:10.1016/j.physrep.2024.03.002 (https://doi.org/10.1016%2Fj.physrep.2024.03.002).
18. Herrman, Rebekah; Lotshaw, Phillip C.; Ostrowski, James; Humble, Travis S.; Siopsis, George (2022-04-26). "Multi-angle quantum approximate optimization algorithm" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9043219). *Scientific Reports*. **12** (1): 6781. arXiv:2109.11455 (https://arxiv.org/abs/2109.11455). Bibcode:2022NatSR..12.6781H (https://ui.adsabs.harvard.edu/abs/2022NatSR..12.6781H). doi:10.1038/s41598-022-10555-8 (https://doi.org/10.1038%2Fs41598-022-10555-8). ISSN 2045-2322 (https://search.worldcat.org/issn/2045-2322). PMC 9043219 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9043219). PMID 35474081 (https://pubmed.ncbi.nlm.nih.gov/35474081).
19. Chalupnik, Michelle; Melo, Hans; Alexeev, Yuri; Galda, Alexey (September 2022). "Augmenting QAOA Ansatz with Multiparameter Problem-Independent Layer" (https://ieeexplore.ieee.org/document/9951267). *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE. pp. 97–103. arXiv:2205.01192 (https://arxiv.org/abs/2205.01192). doi:10.1109/QCE53715.2022.00028 (https://doi.org/10.1109%2FQCE53715.2022.00028). ISBN 978-1-6654-9113-6.
20. Chandarana, P.; Hegade, N. N.; Paul, K.; Albarrán-Arriagada, F.; Solano, E.; del Campo, A.; Chen, Xi (2022-02-22). "Digitized-counterdiabatic quantum approximate optimization algorithm" (https://link.aps.org/doi/10.1103/PhysRevResearch.4.013141). *Physical Review Research*. **4** (1): 013141. arXiv:2107.02789 (https://arxiv.org/abs/2107.02789). Bibcode:2022PhRvR...4a3141C (https://ui.adsabs.harvard.edu/abs/2022PhRvR...4a3141C). doi:10.1103/PhysRevResearch.4.013141 (https://doi.org/10.1103%2FPhysRevResearch.4.013141). ISSN 2643-1564 (https://search.worldcat.org/issn/2643-1564).
21. Hadfield, Stuart; Wang, Zhihui; O'Gorman, Bryan; Rieffel, Eleanor; Venturelli, Davide; Biswas, Rupak (2019-02-12). "From the Quantum Approximate Optimization Algorithm to a Quantum Alternating Operator Ansatz" (https://doi.org/10.3390%2Fa12020034). *Algorithms*. **12** (2): 34. arXiv:1709.03489 (https://arxiv.org/abs/1709.03489). doi:10.3390/a12020034 (https://doi.org/10.3390%2Fa12020034). ISSN 1999-4893 (https://search.worldcat.org/issn/1999-4893).

External links

- Implementation of the QAOA algorithm for the knapsack problem with Classiq (https://short.classiq.io/qaoa_knapsack)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_optimization_algorithms&oldid=1242801584"

WIKIPEDIA
The Free Encyclopedia

Quantum phase estimation algorithm

In quantum computing, the **quantum phase estimation algorithm** is a quantum algorithm to estimate the phase corresponding to an eigenvalue of a given unitary operator. Because the eigenvalues of a unitary operator always have unit modulus, they are characterized by their phase, and therefore the algorithm can be equivalently described as retrieving either the phase or the eigenvalue itself. The algorithm was initially introduced by Alexei Kitaev in 1995.[1][2]:246

Phase estimation is frequently used as a subroutine in other quantum algorithms, such as Shor's algorithm,[2]:131 the quantum algorithm for linear systems of equations, and the quantum counting algorithm.

Overview of the algorithm

The algorithm operates on two sets of qubits, referred to in this context as registers. The two registers contain n and m qubits, respectively. Let U be a unitary operator acting on the m-qubit register. The eigenvalues of a unitary operator have unit modulus, and are therefore characterized by their phase. Thus if $|\psi\rangle$ is an eigenvector of U, then $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$ for some $\theta \in \mathbb{R}$. Due to the periodicity of the complex exponential, we can always assume $0 \leq \theta < 1$.

The goal is producing a good approximation for θ with a small number of gates and a high probability of success. The quantum phase estimation algorithm achieves this assuming oracular access to U, and having $|\psi\rangle$ available as a quantum state. This means that when discussing the efficiency of the algorithm we only worry about the number of times U needs to be used, but not about the cost of implementing U itself.

More precisely, the algorithm returns with high probability an approximation for θ, within additive error ε, using $n = O(\log(1/\varepsilon))$ qubits in the first register, and $O(1/\varepsilon)$ controlled-U operations. Furthermore, we can improve the success probability to $1 - \Delta$ for any $\Delta > 0$ by using a total of $O(\log(1/\Delta)/\varepsilon)$ uses of controlled-U, and this is optimal.[3]

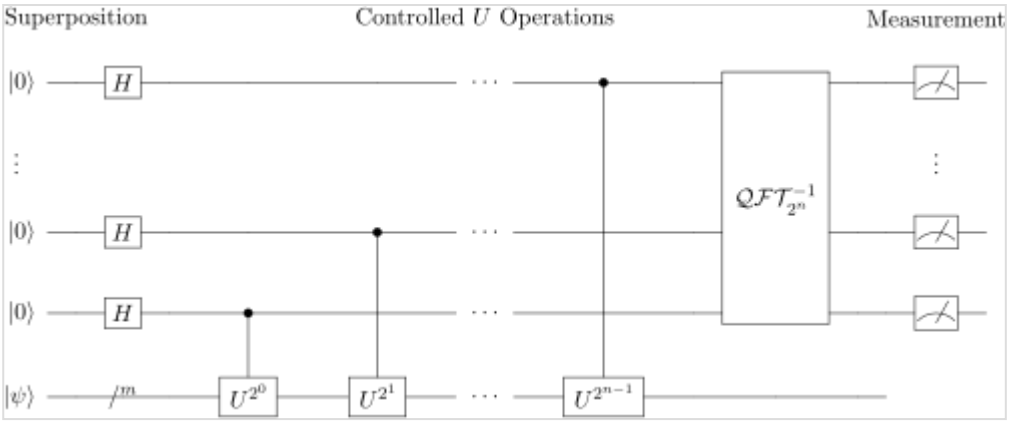
Detailed description of the algorithm

State preparation

The initial state of the system is:

$$|\Psi_0\rangle = |0\rangle^{\otimes n}|\psi\rangle,$$

where $|\psi\rangle$ is the m-qubit state that evolves through U. We first apply the *n-qubit* Hadamard gate operation $H^{\otimes n}$ on the first register, which produces the state:



The circuit for quantum phase estimation.

$$|\Psi_1\rangle = (H^{\otimes n} \otimes I_m)|\Psi_0\rangle = \frac{1}{2^{\frac{n}{2}}}(|0\rangle + |1\rangle)^{\otimes n}|\psi\rangle = \frac{1}{2^{n/2}}\sum_{j=0}^{2^n-1}|j\rangle|\psi\rangle.$$

Note that here we are switching between binary and n-ary representation for the n-qubit register: the ket $|j\rangle$ on the right-hand side is shorthand for the n-qubit state $|j\rangle \equiv \bigotimes_{\ell=0}^{n-1}|j_\ell\rangle$, where $j = \sum_{\ell=0}^{n-1} j_\ell 2^\ell$ is the binary decomposition of j.

Controlled-U operations

This state $|\Psi_1\rangle$ is then evolved through the controlled-unitary evolution U_C whose action can be written as

$$U_C(|k\rangle \otimes |\psi\rangle) = |k\rangle \otimes (U^k|\psi\rangle),$$

for all $k = 0, \ldots, 2^n - 1$. This evolution can also be written concisely as

$$U_C = \sum_{k=0}^{2^n-1}|k\rangle\langle k| \otimes U^k,$$

which highlights its controlled nature: it applies U^k to the second register conditionally to the first register being $|k\rangle$. Remembering the eigenvalue condition holding for $|\psi\rangle$, applying U_C to $|\Psi_1\rangle$ thus gives

$$|\Psi_2\rangle \equiv U_C|\Psi_1\rangle = \left(\frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1}e^{2\pi i\theta k}|k\rangle\right) \otimes |\psi\rangle,$$

where we used $U^k|\psi\rangle = e^{2\pi i k\theta}|\psi\rangle$.

To show that U_C can also be implemented efficiently, observe that we can write $U_C = \prod_{\ell=0}^{n-1} C_\ell(U^{2^\ell})$, where $C_\ell(U^{2^\ell})$ denotes the operation of applying U^{2^ℓ} to the second register conditionally to the ℓ-th qubit of the first register being $|1\rangle$. Formally, these gates can be characterized by their action as

$$C_\ell(U^k)(|j\rangle \otimes |\psi\rangle) = |j\rangle \otimes (U^{j_\ell k}|\psi\rangle).$$

This equation can be interpreted as saying that the state is left unchanged when $j_\ell = 0$, that is, when the ℓ-th qubit is $|0\rangle$, while the gate U^k is applied to the second register when the ℓ-th qubit is $|1\rangle$. The composition of these controlled-gates thus gives

$$\prod_{\ell=0}^{n-1} C_\ell(U^{2^\ell})(|j\rangle \otimes |\psi\rangle) = |j\rangle \otimes \left(U^{\sum_{\ell=0}^{n-1} j_\ell 2^\ell}|\psi\rangle\right) = U_C,$$

with the last step directly following from the binary decomposition $j = \sum_{\ell=0}^{n-1} j_\ell 2^\ell$.

From this point onwards, the second register is left untouched, and thus it is convenient to write $|\Psi_2\rangle = |\tilde{\Psi}_2\rangle \otimes |\psi\rangle$, with $|\tilde{\Psi}_2\rangle$ the state of the n-qubit register, which is the only one we need to consider for the rest of the algorithm.

Apply inverse quantum Fourier transform

The final part of the circuit involves applying the inverse quantum Fourier transform (QFT) $\mathcal{QFT}$ on the first register of $|\Psi_2\rangle$:

$$|\tilde{\Psi}_3\rangle = \mathcal{QFT}_{2^n}^{-1}|\tilde{\Psi}_2\rangle.$$

The QFT and its inverse are characterized by their action on basis states as

$$\mathcal{QFT}_N|k\rangle = N^{-1/2}\sum_{j=0}^{N-1} e^{\frac{2\pi i}{N}jk}|j\rangle,$$
$$\mathcal{QFT}_N^{-1}|k\rangle = N^{-1/2}\sum_{j=0}^{N-1} e^{-\frac{2\pi i}{N}jk}|j\rangle.$$

It follows that

$$|\tilde{\Psi}_3\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e^{2\pi i\theta k}\left(\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1} e^{\frac{-2\pi ikx}{2^n}}|x\rangle\right) = \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{-\frac{2\pi ik}{2^n}(x-2^n\theta)}|x\rangle.$$

Decomposing the state in the computational basis as $|\tilde{\Psi}_3\rangle = \sum_{x=0}^{2^n-1} c_x|x\rangle$, the coefficients thus equal

$$c_x \equiv \frac{1}{2^n}\sum_{k=0}^{2^n-1} e^{-\frac{2\pi ik}{2^n}(x-2^n\theta)} = \frac{1}{2^n}\sum_{k=0}^{2^n-1} e^{-\frac{2\pi ik}{2^n}(x-a)}e^{2\pi i\delta k},$$

where we wrote $2^n\theta = a + 2^n\delta$, with a is the nearest integer to $2^n\theta$. The difference $2^n\delta$ must by definition satisfy $0 \leqslant |2^n\delta| \leqslant \frac{1}{2}$. This amounts to approximating the value of $\theta \in [0, 1]$ by rounding $2^n\theta$ to the nearest integer.

Measurement

The final step involves performing a measurement in the computational basis on the first register. This yields the outcome $|y\rangle$ with probability

$$\Pr(y) = |c_y|^2 = \left| \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{\frac{-2\pi i k}{2^n}(y-a)} e^{2\pi i \delta k} \right|^2.$$

It follows that $\Pr(a) = 1$ if $\delta = 0$, that is, when θ can be written as $\theta = a/2^n$, one always finds the outcome $y = a$. On the other hand, if $\delta \neq 0$, the probability reads

$$\Pr(a) = \frac{1}{2^{2n}} \left| \sum_{k=0}^{2^n-1} e^{2\pi i \delta k} \right|^2 = \frac{1}{2^{2n}} \left| \frac{1 - e^{2\pi i 2^n \delta}}{1 - e^{2\pi i \delta}} \right|^2.$$

From this expression we can see that $\Pr(a) \geqslant \frac{4}{\pi^2} \approx 0.405$ when $\delta \neq 0$. To see this, we observe that from the definition of δ we have the inequality $|\delta| \leqslant \frac{1}{2^{n+1}}$, and thus:[4]:157[5]:348

$$\begin{aligned}
\Pr(a) &= \frac{1}{2^{2n}} \left| \frac{1 - e^{2\pi i 2^n \delta}}{1 - e^{2\pi i \delta}} \right|^2 && \text{for } \delta \neq 0 \\
&= \frac{1}{2^{2n}} \left| \frac{2 \sin(\pi 2^n \delta)}{2 \sin(\pi \delta)} \right|^2 && \left|1 - e^{2ix}\right|^2 = 4|\sin(x)|^2 \\
&= \frac{1}{2^{2n}} \frac{|\sin(\pi 2^n \delta)|^2}{|\sin(\pi \delta)|^2} \\
&\geqslant \frac{1}{2^{2n}} \frac{|\sin(\pi 2^n \delta)|^2}{|\pi \delta|^2} && |\sin(\pi\delta)| \leqslant |\pi\delta| \\
&\geqslant \frac{1}{2^{2n}} \frac{|2 \cdot 2^n \delta|^2}{|\pi \delta|^2} && |2 \cdot 2^n \delta| \leqslant |\sin(\pi 2^n \delta)| \text{ for } |\delta| \leqslant \frac{1}{2^{n+1}} \\
&\geqslant \frac{4}{\pi^2}.
\end{aligned}$$

We conclude that the algorithm provides the best n-bit estimate (i.e., one that is within $1/2^n$ of the correct answer) of θ with probability at least $4/\pi^2$. By adding a number of extra qubits on the order of $O(\log(1/\epsilon))$ and truncating the extra qubits the probability can increase to $1 - \epsilon$.[5]

Toy examples

Consider the simplest possible instance of the algorithm, where only $n = 1$ qubit, on top of the qubits required to encode $|\psi\rangle$, is involved. Suppose the eigenvalue of $|\psi\rangle$ reads $\lambda = e^{2\pi i \theta}$, $\theta \in [0, 1)$. The first part of the algorithm generates the one-qubit state $|\phi\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + \lambda|1\rangle)$. Applying the inverse QFT

amounts in this case to applying a Hadamard gate. The final outcome probabilities are thus $p_\pm = |\langle \pm | \phi \rangle|^2$ where $|\pm\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, or more explicitly,

$$p_\pm = \frac{|1 \pm \lambda|^2}{4} = \frac{1 \pm \cos(2\pi\theta)}{2}.$$

Suppose $\lambda = 1$, meaning $|\phi\rangle = |+\rangle$. Then $p_+ = 1$, $p_- = 0$, and we recover deterministically the precise value of λ from the measurement outcomes. The same applies if $\lambda = -1$.

If on the other hand $\lambda = e^{2\pi i/3}$, then $p_\pm = [1 \pm \cos(2\pi/3)]/2$, that is, $p_+ = 1/4$ and $p_- = 3/4$. In this case the result is not deterministic, but we still find the outcome $|-\rangle$ as more likely, compatibly with the fact that $2/3$ is closer to 1 than to 0.

More generally, if $\lambda = e^{2\pi i\theta}$, then $p_+ \geq 1/2$ if and only if $|\theta| \leq 1/4$. This is consistent with the results above because in the cases $\lambda = \pm 1$, corresponding to $\theta = 0, 1/2$, the phase is retrieved deterministically, and the other phases are retrieved with higher accuracy the closer they are to these two.

See also

- Shor's algorithm
- Quantum counting algorithm
- Parity measurement

References

1. Kitaev, A. Yu (1995-11-20). "Quantum measurements and the Abelian Stabilizer Problem". arXiv:quant-ph/9511026 (https://arxiv.org/abs/quant-ph/9511026).
2. Nielsen, Michael A. & Isaac L. Chuang (2001). *Quantum computation and quantum information* (Repr. ed.). Cambridge [u.a.]: Cambridge Univ. Press. ISBN 978-0521635035.
3. Mande, Nikhil S.; Ronald de Wolf (2023). "Tight Bounds for Quantum Phase Estimation and Related Problems". arXiv:2305.04908 (https://arxiv.org/abs/2305.04908) [quant-ph (https://arxiv.org/archive/quant-ph)].
4. Benenti, Guiliano; Casati, Giulio; Strini, Giuliano (2004). *Principles of quantum computation and information* (Reprinted. ed.). New Jersey [u.a.]: World Scientific. ISBN 978-9812388582.
5. Cleve, R.; Ekert, A.; Macchiavello, C.; Mosca, M. (8 January 1998). "Quantum algorithms revisited". *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. **454** (1969): 339–354. arXiv:quant-ph/9708016 (https://arxiv.org/abs/quant-ph/9708016). Bibcode:1998RSPSA.454..339C (https://ui.adsabs.harvard.edu/abs/1998RSPSA.454..339C). doi:10.1098/rspa.1998.0164 (https://doi.org/10.1098%2Frspa.1998.0164). S2CID 16128238 (https://api.semanticscholar.org/CorpusID:16128238).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_phase_estimation_algorithm&oldid=1241231130"

WIKIPEDIA
The Free Encyclopedia

Shor's algorithm

Shor's algorithm is a quantum algorithm for finding the prime factors of an integer. It was developed in 1994 by the American mathematician Peter Shor.[1][2] It is one of the few known quantum algorithms with compelling potential applications and strong evidence of superpolynomial speedup compared to best known classical (non-quantum) algorithms.[3] On the other hand, factoring numbers of practical significance requires far more qubits than available in the near future.[4] Another concern is that noise in quantum circuits may undermine results,[5] requiring additional qubits for quantum error correction.

Shor proposed multiple similar algorithms for solving the factoring problem, the discrete logarithm problem, and the period-finding problem. "Shor's algorithm" usually refers to the factoring algorithm, but may refer to any of the three algorithms. The discrete logarithm algorithm and the factoring algorithm are instances of the period-finding algorithm, and all three are instances of the hidden subgroup problem.

On a quantum computer, to factor an integer N, Shor's algorithm runs in polynomial time, meaning the time taken is polynomial in $\log N$.[6] It takes quantum gates of order $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$ using fast multiplication,[7] or even $O\left((\log N)^2(\log\log N)\right)$ utilizing the asymptotically fastest multiplication algorithm currently known due to Harvey and Van Der Hoven,[8] thus demonstrating that the integer factorization problem can be efficiently solved on a quantum computer and is consequently in the complexity class **BQP**. This is significantly faster than the most efficient known classical factoring algorithm, the general number field sieve, which works in sub-exponential time: $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$.[9]

Feasibility and impact

If a quantum computer with a sufficient number of qubits could operate without succumbing to quantum noise and other quantum-decoherence phenomena, then Shor's algorithm could be used to break public-key cryptography schemes, such as

- The RSA scheme
- The Finite Field Diffie-Hellman key exchange
- The Elliptic Curve Diffie-Hellman key exchange[10]

RSA is based on the assumption that factoring large integers is computationally intractable. As far as is known, this assumption is valid for classical (non-quantum) computers; no classical algorithm is known that can factor integers in polynomial time. However, Shor's algorithm shows that factoring integers is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by constructing a large quantum computer. It was also a powerful motivator for the design and construction of quantum computers, and for the study of new quantum-computer algorithms. It has also facilitated research on new cryptosystems that are secure from quantum computers, collectively called post-quantum cryptography.

Physical implementation

Given the high error rates of contemporary quantum computers and too few qubits to use quantum error correction, laboratory demonstrations obtain correct results only in a fraction of attempts.

In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3×5, using an NMR implementation of a quantum computer with seven qubits.[11] After IBM's implementation, two independent groups implemented Shor's algorithm using photonic qubits, emphasizing that multi-qubit entanglement was observed when running the Shor's algorithm circuits.[12][13] In 2012, the factorization of 15 was performed with solid-state qubits.[14] Later, in 2012, the factorization of 21 was achieved.[15] In 2016, the factorization of 15 was performed again using trapped-ion qubits with a recycling technique.[16] In 2019, an attempt was made to factor the number 35 using Shor's algorithm on an IBM Q System One, but the algorithm failed because of accumulating errors.[17] However, all these demonstrations have compiled the algorithm by making use of prior knowledge of the answer, and some have even oversimplified the algorithm in a way that makes it equivalent to coin flipping.[18] Furthermore, attempts using quantum computers with other algorithms have been made.[19] However, these algorithms are similar to classical brute-force checking of factors, so unlike Shor's algorithm, they are not expected to ever perform better than classical factoring algorithms.[20]

Theoretical analyses of Shor's algorithm assume a quantum computer free of noise and errors. However, near-term practical implementations will have to deal with such undesired phenomena (when more qubits are available, Quantum error correction can help). In 2023, Jin-Yi Cai showed that in the presence of noise, Shor's algorithm fails asymptotically almost surely for large semiprimes that are products of two primes in OEIS sequence A073024 (https://oeis.org/A073024).[5] These primes p have the property that $p-1$ has a prime factor larger than $p^{2/3}$, and have a positive density in the set of all primes. Hence error-correction will be needed to be able to factor all numbers with Shor's algorithm.

Algorithm

The problem that we are trying to solve is: *given an odd composite number N, find its integer factors*.

To achieve this, Shor's algorithm consists of two parts:

1. A classical reduction of the factoring problem to the problem of order-finding. This reduction is similar to that used for other factoring algorithms, such as the quadratic sieve.
2. A quantum algorithm to solve the order-finding problem.

Classical reduction

A complete factoring algorithm is possible if we're able to efficiently factor arbitrary N into just two integers p and q greater than 1, since if either p or q are not prime then the factoring algorithm can in turn be run on those until only primes remain.

A basic observation is that, using Euclid's algorithm, we can always compute the GCD between two integers efficiently. In particular, this means we can check efficiently whether N is even, in which case 2 is trivially a factor. Let us thus assume that N is odd for the remainder of this discussion. Afterwards, we can use efficient classical algorithms to check if N is a prime power.[21] For prime powers, efficient classical factorization algorithms exist,[22] hence the rest of the quantum algorithm may assume that N is not a prime power.

If those easy cases do not produce a nontrivial factor of N, the algorithm proceeds to handle the remaining case. We pick a random integer $2 \leq a < N$. A possible nontrivial divisor of N can be found by computing $\gcd(a, N)$, which can be done classically and efficiently using the Euclidean algorithm. If this produces a nontrivial factor (meaning $\gcd(a, N) \neq 1$), the algorithm is finished, and the other nontrivial factor is $\frac{N}{\gcd(a,N)}$. If a nontrivial factor was not identified, then that means that N and the choice of a are coprime, so a is contained in the multiplicative group of integers modulo N, having a multiplicative inverse modulo N. Thus, a has a multiplicative order r modulo N, meaning

$$a^r \equiv 1 \bmod N$$

and r is the smallest positive integer satisfying this congruence.

The quantum subroutine finds r. It can be seen from the congruence that N divides $a^r - 1$, written $N \mid a^r - 1$. This can be factored using difference of squares:

$$N \mid (a^{r/2} - 1)(a^{r/2} + 1)$$

Since we have factored the expression in this way, the algorithm doesn't work for odd r (because $a^{r/2}$ must be an integer), meaning the algorithm would have to restart with a new a. Hereafter we can therefore assume r is even. It cannot be the case that $N \mid a^{r/2} - 1$, since this would imply $a^{r/2} \equiv 1 \bmod N$, which would contradictorily imply that $\frac{r}{2}$ would be the order of a, which was already r. At this point, it may or may not be the case that $N \mid a^{r/2} + 1$. If it is not true that $N \mid a^{r/2} + 1$, then that means we are able to find a nontrivial factor of N. We compute

$$d = \gcd(N, a^{r/2} - 1)$$

If $d = 1$, then that means $N \mid a^{r/2} + 1$ was true, and a nontrivial factor of N cannot be achieved from a, and the algorithm must restart with a new a. Otherwise, we have found a nontrivial factor of N, with the other being $\frac{N}{d}$, and the algorithm is finished. For this step, it is also equivalent to compute $\gcd(N, a^{r/2} + 1)$; it will produce a nontrivial factor if $\gcd(N, a^{r/2} - 1)$ is nontrivial, and will not if it's trivial (where $N \mid a^{r/2} + 1$).

The algorithm restated shortly follows: let N be odd, and not a prime power. We want to output two nontrivial factors of N.

1. Pick a random number $1 < a < N$.
2. Compute $K = \gcd(a, N)$, the greatest common divisor of a and N.
3. If $K \neq 1$, then K is a nontrivial factor of N, with the other factor being $\frac{N}{K}$ and we are done.
4. Otherwise, use the quantum subroutine to find the order r of a.
5. If r is odd, then go back to step 1.
6. Compute $g = \gcd(N, a^{r/2} + 1)$. If g is nontrivial, the other factor is $\frac{N}{g}$, and we're done. Otherwise, go back to step 1.

It has been shown that this will be likely to succeed after a few runs.[2] In practice, a single call to the quantum order-finding subroutine is enough to completely factor N with very high probability of success if one uses a more advanced reduction.[23]

Quantum order-finding subroutine

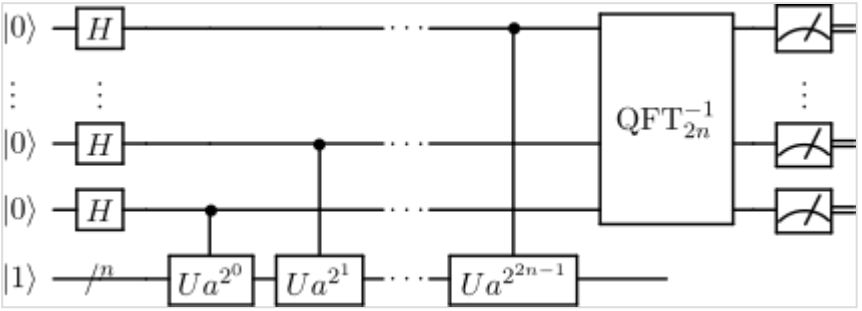
The goal of the quantum subroutine of Shor's algorithm is, given coprime integers N and $1 < a < N$, to find the order r of a modulo N, which is the smallest positive integer such that $a^r \equiv 1 \pmod{N}$. To achieve this, Shor's algorithm uses a quantum circuit involving two registers. The second register uses n qubits, where n is the smallest integer such that $N \leq 2^n$, i.e., $n = \lceil \log_2 N \rceil$. The size of the first register determines how accurate of an approximation the circuit produces. It can be shown that using $2n + 1$ qubits gives sufficient accuracy to find r. The exact quantum circuit depends on the parameters a and N, which define the problem. The following description of the algorithm uses bra–ket notation to denote quantum states, and $\otimes$ to denote the tensor product, rather than logical AND.

The algorithm consists of two main steps:

1. Use quantum phase estimation with unitary U representing the operation of multiplying by a (modulo N), and input state $|0\rangle^{\otimes 2n+1} \otimes |1\rangle$ (where the second register is $|1\rangle$ made from n qubits). The eigenvalues of this U encode information about the period, and $|1\rangle$ can be seen to be writable as a sum of its eigenvectors. Thanks to these properties, the quantum phase estimation stage gives as output a random integer of the form $\frac{j}{r} 2^{2n+1}$ for random $j = 0, 1, \ldots, r-1$.
2. Use the continued fractions algorithm to extract the period r from the measurement outcomes obtained in the previous stage. This is a procedure to post-process (with a classical computer) the measurement data obtained from measuring the output quantum states, and retrieve the period.

The connection with quantum phase estimation was not discussed in the original formulation of Shor's algorithm,[2] but was later proposed by Kitaev.[24]

Quantum phase estimation



Quantum subroutine in Shor's algorithm

In general the quantum phase estimation algorithm, for any unitary U and eigenstate $|\psi\rangle$ such that $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$, sends input states $|0\rangle|\psi\rangle$ to output states close to $|\phi\rangle|\psi\rangle$, where ϕ is an integer close to $2^{2n+1}\theta$. In other words, it sends each eigenstate $|\psi_j\rangle$ of U to a state close to the associated eigenvalue.

For the purposes of quantum order-finding, we employ this strategy using the unitary defined by the action

$$U|k\rangle = \begin{cases} |ak \pmod N\rangle & 0 \leq k < N, \\ |k\rangle & N \leq k < 2^n. \end{cases}$$

The action of U on states $|k\rangle$ with $N \leq k < 2^n$ is not crucial to the functioning of the algorithm, but needs to be included to ensure the overall transformation is a well-defined quantum gate. Implementing the circuit for quantum phase estimation with U requires being able to efficiently implement the gates U^{2^j}. This can be accomplished via modular exponentiation, which is the slowest part of the algorithm. The gate thus defined satisfies $U^r = I$, which immediately implies that its eigenvalues are the r-th roots of unity $\omega_r^k = e^{2\pi i k/r}$. Furthermore, each eigenvalue ω_r^j has an eigenvector of the form $|\psi_j\rangle = r^{-1/2} \sum_{k=0}^{r-1} \omega_r^{-kj} |a^k\rangle$, and these eigenvectors are such that

$$\begin{aligned} \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\psi_j\rangle &= \frac{1}{r} \sum_{j=0}^{r-1} \sum_{k=0}^{r-1} \omega_r^{jk} |a^k\rangle \\ &= |1\rangle + \frac{1}{r} \sum_{k=1}^{r-1} \left(\sum_{j=0}^{r-1} \omega_r^{jk} \right) |a^k\rangle = |1\rangle, \end{aligned}$$

where the last identity follows from the geometric series formula, which implies $\sum_{j=0}^{r-1} \omega_r^{jk} = 0$.

Using quantum phase estimation on an input state $|0\rangle^{\otimes 2n+1} |\psi_j\rangle$ would then return the integer $2^{2n+1} j/r$ with high probability. More precisely, the quantum phase estimation circuit sends $|0\rangle^{\otimes 2n+1} |\psi_j\rangle$ to $|\phi_j\rangle |\psi_j\rangle$ such that the resulting probability distribution $p_k \equiv |\langle k|\phi_j\rangle|^2$ is peaked around $k = 2^{2n+1} j/r$, with $p_{2^{2n+1} j/r} \geq \frac{4}{\pi^2} \approx 0.4053$. This probability can be made arbitrarily close to 1 using extra qubits.

Applying the above reasoning to the input $|0\rangle^{\otimes 2n+1} |1\rangle$, quantum phase estimation thus results in the evolution

$$|0\rangle^{\otimes 2n} |1\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |0\rangle^{\otimes 2n} |\psi_j\rangle \to \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\phi_j\rangle |\psi_j\rangle.$$

Measuring the first register, we now have a balanced probability $1/r$ to find each $|\phi_j\rangle$, each one giving an integer approximation to $2^{2n+1} j/r$, which can be divided by 2^{2n+1} to get a decimal approximation for j/r.

Continued fraction algorithm to retrieve the period

Then, we apply the continued fractions algorithm to find integers b and c, where $\frac{b}{c}$ gives the best fraction approximation for the approximation measured from the circuit, for $b, c < N$ and coprime b and c. The number of qubits in the first register, $2n + 1$, which determines the accuracy of the approximation, guarantees that

$$\frac{b}{c} = \frac{j}{r}$$

given the best approximation from the superposition of $|\phi_j\rangle$ was measured[2] (which can be made arbitrarily likely by using extra bits and truncating the output). However, while b and c are coprime, it may be the case that j and r are not coprime. Because of that, b and c may have lost some factors that were in j and r. This can be remedied by rerunning the quantum order-finding subroutine an arbitrary number of times, to produce a list of fraction approximations

$$\frac{b_1}{c_1}, \frac{b_2}{c_2}, \cdots, \frac{b_s}{c_s}$$

where s is the number of times the subroutine was run. Each c_k will have different factors taken out of it because the circuit will (likely) have measured multiple different possible values of j. To recover the actual r value, we can take the least common multiple of each c_k:

$$\operatorname{lcm}(c_1, c_2, \ldots, c_s)$$

The least common multiple will be the order r of the original integer a with high probability. In practice, a single run of the quantum order-finding subroutine is in general enough if more advanced post-processing is used.[25]

Choosing the size of the first register

Phase estimation requires choosing the size of the first register to determine the accuracy of the algorithm, and for the quantum subroutine of Shor's algorithm, $2n+1$ qubits is sufficient to guarantee that the optimal bitstring measured from phase estimation (meaning the $|k\rangle$ where $k/2^{2n+1}$ is the most accurate approximation of the phase from phase estimation) will allow the actual value of r to be recovered.

Each $|\phi_j\rangle$ before measurement in Shor's algorithm represents a superposition of integers approximating $2^{2n+1}j/r$. Let $|k\rangle$ represent the most optimal integer in $|\phi_j\rangle$. The following theorem guarantees that the continued fractions algorithm will recover j/r from $k/2^{2n+1}$:

> **Theorem** — If j and r are n bit integers, and
>
> $$\left|\frac{j}{r} - \phi\right| \leq \frac{1}{2r^2}$$
>
> then the continued fractions algorithm run on ϕ will recover both $\frac{j}{\gcd(j,\, r)}$ and $\frac{r}{\gcd(j,\, r)}$.

[3] As k is the optimal bitstring from phase estimation, $k/2^{2n+1}$ is accurate to j/r by $2n+1$ bits. Thus,

$$\left|\frac{j}{r} - \frac{k}{2^{2n+1}}\right| \leq \frac{1}{2^{2n+1}} \leq \frac{1}{2N^2} \leq \frac{1}{2r^2}$$

which implies that the continued fractions algorithm will recover j and r (or with their greatest common divisor taken out).

The bottleneck

The runtime bottleneck of Shor's algorithm is quantum modular exponentiation, which is by far slower than the quantum Fourier transform and classical pre-/post-processing. There are several approaches to constructing and optimizing circuits for modular exponentiation. The simplest and (currently) most practical approach is to mimic conventional arithmetic circuits with reversible gates, starting with ripple-carry adders. Knowing the base and the modulus of exponentiation facilitates further optimizations.[26][27] Reversible circuits typically use on the order of n^3 gates for n qubits. Alternative techniques asymptotically improve gate counts by using quantum Fourier transforms, but are not competitive with fewer than 600 qubits owing to high constants.

Period finding and discrete logarithms

Shor's algorithms for the discrete log and the order finding problems are instances of an algorithm solving the period finding problem.. All three are instances of the hidden subgroup problem.

Shor's algorithm for discrete logarithms

Given a group G with order p and generator $g \in G$, suppose we know that $x = g^r \in G$, for some $r \in \mathbb{Z}_p$, and we wish to compute r, which is the discrete logarithm: $r = \log_g(x)$. Consider the abelian group $\mathbb{Z}_p \times \mathbb{Z}_p$, where each factor corresponds to modular addition of values. Now, consider the function

$$f\colon \mathbb{Z}_p \times \mathbb{Z}_p \to G\ ;\ f(a,b) = g^a x^{-b}.$$

This gives us an abelian hidden subgroup problem, where f corresponds to a group homomorphism. The kernel corresponds to the multiples of $(r, 1)$. So, if we can find the kernel, we can find r. A quantum algorithm for solving this problem exists. This algorithm is, like the factor-finding algorithm, due to Peter Shor and both are implemented by creating a superposition through using Hadamard gates, followed by implementing f as a quantum transform, followed finally by a quantum Fourier transform.[3] Due to this, the quantum algorithm for computing the discrete logarithm is also occasionally referred to as "Shor's Algorithm."

The order-finding problem can also be viewed as a hidden subgroup problem.[3] To see this, consider the group of integers under addition, and for a given $a \in \mathbb{Z}$ such that: $a^r = 1$, the function

$$f\colon \mathbb{Z} \to \mathbb{Z}\ ;\ f(x) = a^x,\ f(x + r) = f(x).$$

For any finite abelian group G, a quantum algorithm exists for solving the hidden subgroup for G in polynomial time.[3]

See also

- GEECM, a factorization algorithm said to be "often much faster than Shor's"[28]
- Grover's algorithm

References

1. Shor, P.W. (1994). "Algorithms for quantum computation: Discrete logarithms and factoring". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. pp. 124–134. doi:10.1109/sfcs.1994.365700 (https://doi.org/10.1109%2Fsfcs.1994.365700). ISBN 978-0-8186-6580-6.
2. Shor, Peter W. (October 1997). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal on Computing*. **26** (5): 1484–1509. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). doi:10.1137/S0097539795293172 (https://doi.org/10.1137%2FS0097539795293172). S2CID 2337707 (https://api.semanticscholar.org/CorpusID:2337707).
3. Nielsen, Michael A.; Chuang, Isaac L. (9 December 2010). *Quantum Computation and Quantum Information* (http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf) (PDF) (7th ed.). Cambridge University Press. ISBN 978-1-107-00217-3. Archived (https://web.archive.org/web/20190711070716/http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf) (PDF) from the original on 2019-07-11. Retrieved 24 April 2022.
4. Gidney, Craig; Ekerå, Martin (2021). "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". *Quantum*. **5**: 433. arXiv:1905.09749 (https://arxiv.org/abs/1905.09749). Bibcode:2021Quant...5..433G (https://ui.adsabs.harvard.edu/abs/2021Quant...5..433G). doi:10.22331/q-2021-04-15-433 (https://doi.org/10.22331%2Fq-2021-04-15-433). S2CID 162183806 (https://api.semanticscholar.org/CorpusID:162183806).
5. Cai, Jin-Yi (2024). "Shor's algorithm does not factor large integers in the presence of noise". *Science China Information Sciences*. **67** (7). arXiv:2306.10072 (https://arxiv.org/abs/2306.10072). doi:10.1007/s11432-023-3961-3 (https://doi.org/10.1007%2Fs11432-023-3961-3).
6. See also pseudo-polynomial time.
7. Beckman, David; Chari, Amalavoyal N.; Devabhaktuni, Srikrishna; Preskill, John (August 1996). "Efficient networks for quantum factoring". *Physical Review A*. **54** (2): 1034–1063. arXiv:quant-ph/9602016 (https://arxiv.org/abs/quant-ph/9602016). Bibcode:1996PhRvA..54.1034B (https://ui.adsabs.harvard.edu/abs/1996PhRvA..54.1034B). doi:10.1103/physreva.54.1034 (https://doi.org/10.1103%2Fphysreva.54.1034). PMID 9913575 (https://pubmed.ncbi.nlm.nih.gov/9913575).
8. Harvey, David; van der Hoeven, Joris (March 2021). "Integer multiplication in time O (n log n)" (https://hal.science/hal-02070778v2/file/nlogn.pdf) (PDF). *Annals of Mathematics*. **193** (2). doi:10.4007/annals.2021.193.2.4 (https://doi.org/10.4007%2Fannals.2021.193.2.4).
9. "Number Field Sieve" (http://mathworld.wolfram.com/NumberFieldSieve.html). *wolfram.com*. Retrieved 23 October 2015.
10. Roetteler, Martin; Naehrig, Michael; Svore, Krysta M.; Lauter, Kristin E. (2017). "Quantum resource estimates for computing elliptic curve discrete logarithms". In Takagi, Tsuyoshi; Peyrin, Thomas (eds.). *Advances in Cryptology – ASIACRYPT 2017 – 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3–7, 2017, Proceedings, Part II*. Lecture Notes in Computer Science. Vol. 10625. Springer. pp. 241–270. arXiv:1706.06752 (https://arxiv.org/abs/1706.06752). doi:10.1007/978-3-319-70697-9_9 (https://doi.org/10.1007%2F978-3-319-70697-9_9). ISBN 978-3-319-70696-2.
11. Vandersypen, Lieven M. K.; Steffen, Matthias; Breyta, Gregory; Yannoni, Costantino S.; Sherwood, Mark H.; Chuang, Isaac L. (December 2001). "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". *Nature*. **414** (6866): 883–887. arXiv:quant-ph/0112176 (https://arxiv.org/abs/quant-ph/0112176). Bibcode:2001Natur.414..883V (https://ui.adsabs.harvard.edu/abs/2001Natur.414..883V). doi:10.1038/414883a (https://doi.org/10.1038%2F414883a). PMID 11780055 (https://pubmed.ncbi.nlm.nih.gov/11780055).

12. Lu, Chao-Yang; Browne, Daniel E.; Yang, Tao; Pan, Jian-Wei (19 December 2007). "Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits". *Physical Review Letters*. **99** (25): 250504. arXiv:0705.1684 (https://arxiv.org/abs/0705.1684). Bibcode:2007PhRvL..99y0504L (https://ui.adsabs.harvard.edu/abs/2007PhRvL..99y0504L). doi:10.1103/PhysRevLett.99.250504 (https://doi.org/10.1103%2FPhysRevLett.99.250504). PMID 18233508 (https://pubmed.ncbi.nlm.nih.gov/18233508).
13. Lanyon, B. P.; Weinhold, T. J.; Langford, N. K.; Barbieri, M.; James, D. F. V.; Gilchrist, A.; White, A. G. (19 December 2007). "Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement". *Physical Review Letters*. **99** (25): 250505. arXiv:0705.1398 (https://arxiv.org/abs/0705.1398). Bibcode:2007PhRvL..99y0505L (https://ui.adsabs.harvard.edu/abs/2007PhRvL..99y0505L). doi:10.1103/PhysRevLett.99.250505 (https://doi.org/10.1103%2FPhysRevLett.99.250505). PMID 18233509 (https://pubmed.ncbi.nlm.nih.gov/18233509).
14. Lucero, Erik; Barends, Rami; Chen, Yu; Kelly, Julian; Mariantoni, Matteo; Megrant, Anthony; O'Malley, Peter; Sank, Daniel; Vainsencher, Amit; Wenner, James; White, Ted; Yin, Yi; Cleland, Andrew N.; Martinis, John M. (2012). "Computing prime factors with a Josephson phase qubit quantum processor". *Nature Physics*. **8** (10): 719. arXiv:1202.5707 (https://arxiv.org/abs/1202.5707). Bibcode:2012NatPh...8..719L (https://ui.adsabs.harvard.edu/abs/2012NatPh...8..719L). doi:10.1038/nphys2385 (https://doi.org/10.1038%2Fnphys2385). S2CID 44055700 (https://api.semanticscholar.org/CorpusID:44055700).
15. Martín-López, Enrique; Martín-López, Enrique; Laing, Anthony; Lawson, Thomas; Alvarez, Roberto; Zhou, Xiao-Qi; O'Brien, Jeremy L. (12 October 2012). "Experimental realization of Shor's quantum factoring algorithm using qubit recycling". *Nature Photonics*. **6** (11): 773–776. arXiv:1111.4147 (https://arxiv.org/abs/1111.4147). Bibcode:2012NaPho...6..773M (https://ui.adsabs.harvard.edu/abs/2012NaPho...6..773M). doi:10.1038/nphoton.2012.259 (https://doi.org/10.1038%2Fnphoton.2012.259). S2CID 46546101 (https://api.semanticscholar.org/CorpusID:46546101).
16. Monz, Thomas; Nigg, Daniel; Martinez, Esteban A.; Brandl, Matthias F.; Schindler, Philipp; Rines, Richard; Wang, Shannon X.; Chuang, Isaac L.; Blatt, Rainer (4 March 2016). "Realization of a scalable Shor algorithm". *Science*. **351** (6277): 1068–1070. arXiv:1507.08852 (https://arxiv.org/abs/1507.08852). Bibcode:2016Sci...351.1068M (https://ui.adsabs.harvard.edu/abs/2016Sci...351.1068M). doi:10.1126/science.aad9480 (https://doi.org/10.1126%2Fscience.aad9480). PMID 26941315 (https://pubmed.ncbi.nlm.nih.gov/26941315). S2CID 17426142 (https://api.semanticscholar.org/CorpusID:17426142).
17. Amico, Mirko; Saleem, Zain H.; Kumph, Muir (8 July 2019). "Experimental study of Shor's factoring algorithm using the IBM Q Experience". *Physical Review A*. **100** (1): 012305. arXiv:1903.00768 (https://arxiv.org/abs/1903.00768). Bibcode:2019PhRvA.100a2305A (https://ui.adsabs.harvard.edu/abs/2019PhRvA.100a2305A). doi:10.1103/PhysRevA.100.012305 (https://doi.org/10.1103%2FPhysRevA.100.012305). S2CID 92987546 (https://api.semanticscholar.org/CorpusID:92987546).
18. Smolin, John A.; Smith, Graeme; Vargo, Alexander (July 2013). "Oversimplifying quantum factoring". *Nature*. **499** (7457): 163–165. arXiv:1301.7007 (https://arxiv.org/abs/1301.7007). Bibcode:2013Natur.499..163S (https://ui.adsabs.harvard.edu/abs/2013Natur.499..163S). doi:10.1038/nature12290 (https://doi.org/10.1038%2Fnature12290). PMID 23846653 (https://pubmed.ncbi.nlm.nih.gov/23846653).
19. Karamlou, Amir H.; Simon, William A.; Katabarwa, Amara; Scholten, Travis L.; Peropadre, Borja; Cao, Yudong (28 October 2021). "Analyzing the performance of variational quantum factoring on a superconducting quantum processor". *npj Quantum Information*. **7** (1): 156. arXiv:2012.07825 (https://arxiv.org/abs/2012.07825). Bibcode:2021npjQI...7..156K (https://ui.adsabs.harvard.edu/abs/2021npjQI...7..156K). doi:10.1038/s41534-021-00478-z (https://doi.org/10.1038%2Fs41534-021-00478-z).
20. "Quantum computing motte-and-baileys" (https://scottaaronson.blog/?p=4447). *Shtetl-Optimized*. 2019-12-28. Retrieved 2021-11-15.

21. Bernstein, Daniel (1998). "Detecting perfect powers in essentially linear time". *Mathematics of Computation*. **67** (223): 1253–1283. doi:10.1090/S0025-5718-98-00952-1 (https://doi.org/10.1090%2FS0025-5718-98-00952-1).
22. e.g., computing the first $\log_2(N)$ roots of N, e.g., with the Newton method and checking each integer result for primality (AKS primality test).
23. Ekerå, Martin (June 2021). "On completely factoring any integer efficiently in a single run of an order-finding algorithm" (https://doi.org/10.1007%2Fs11128-021-03069-1). *Quantum Information Processing*. **20** (6): 205. arXiv:2007.10044 (https://arxiv.org/abs/2007.10044). Bibcode:2021QuIP...20..205E (https://ui.adsabs.harvard.edu/abs/2021QuIP...20..205E). doi:10.1007/s11128-021-03069-1 (https://doi.org/10.1007%2Fs11128-021-03069-1).
24. Kitaev, A. Yu (1995). "Quantum measurements and the Abelian Stabilizer Problem". arXiv:quant-ph/9511026 (https://arxiv.org/abs/quant-ph/9511026).
25. Ekerå, Martin (May 2024). "On the Success Probability of Quantum Order Finding" (https://doi.org/10.1145%2F3655026). *ACM Transactions on Quantum Computing*. **5** (2): 1–40. arXiv:2201.07791 (https://arxiv.org/abs/2201.07791). doi:10.1145/3655026 (https://doi.org/10.1145%2F3655026).
26. Markov, Igor L.; Saeedi, Mehdi (2012). "Constant-Optimized Quantum Circuits for Modular Multiplication and Exponentiation". *Quantum Information and Computation*. **12** (5–6): 361–394. arXiv:1202.6614 (https://arxiv.org/abs/1202.6614). Bibcode:2012arXiv1202.6614M (https://ui.adsabs.harvard.edu/abs/2012arXiv1202.6614M). doi:10.26421/QIC12.5-6-1 (https://doi.org/10.26421%2FQIC12.5-6-1). S2CID 16595181 (https://api.semanticscholar.org/CorpusID:16595181).
27. Markov, Igor L.; Saeedi, Mehdi (2013). "Faster Quantum Number Factoring via Circuit Synthesis". *Phys. Rev. A*. **87** (1): 012310. arXiv:1301.3210 (https://arxiv.org/abs/1301.3210). Bibcode:2013PhRvA..87a2310M (https://ui.adsabs.harvard.edu/abs/2013PhRvA..87a2310M). doi:10.1103/PhysRevA.87.012310 (https://doi.org/10.1103%2FPhysRevA.87.012310). S2CID 2246117 (https://api.semanticscholar.org/CorpusID:2246117).
28. Bernstein, Daniel J.; Heninger, Nadia; Lou, Paul; Valenta, Luke (2017). "Post-quantum RSA". *Post-Quantum Cryptography*. Lecture Notes in Computer Science. Vol. 10346. pp. 311–329. doi:10.1007/978-3-319-59879-6_18 (https://doi.org/10.1007%2F978-3-319-59879-6_18). ISBN 978-3-319-59878-9.

Further reading

- Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press. ISBN 978-1-107-00217-3.
- Kaye, Phillip; Laflamme, Raymond; Mosca, Michele (2006). *An Introduction to Quantum Computing*. doi:10.1093/oso/9780198570004.001.0001 (https://doi.org/10.1093%2Foso%2F9780198570004.001.0001). ISBN 978-0-19-857000-4.
- "Explanation for the man in the street" (http://scottaaronson.com/blog/?p=208) by Scott Aaronson, "approved (http://scottaaronson.com/blog/?p=208#comment-9958)" by Peter Shor. (Shor wrote "Great article, Scott! That's the best job of explaining quantum computing to the man on the street that I've seen."). An alternate metaphor for the QFT was presented in one of the comments (http://www.scottaaronson.com/blog/?p=208#comment-5187). Scott Aaronson suggests the following 12 references as further reading (out of "the $10^{10^{5000}}$ quantum algorithm tutorials that are already on the web."):
- Shor, Peter W. (1997), "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", *SIAM J. Comput.*, **26** (5): 1484–1509, arXiv:quant-ph/9508027v2 (https://arxiv.org/abs/quant-ph/9508027v2), Bibcode:1999SIAMR..41..303S (https://ui.adsabs.harvard.edu/abs/1999SIAMR..41..303S),

doi:10.1137/S0036144598347011 (https://doi.org/10.1137%2FS0036144598347011). Revised version of the original paper by Peter Shor ("28 pages, LaTeX. This is an expanded version of a paper that appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20--22, 1994. Minor revisions made January, 1996").

- Quantum Computing and Shor's Algorithm (https://quantum-algorithms.herokuapp.com/299/paper/index.html), Matthew Hayward's Quantum Algorithms Page (https://quantum-algorithms.herokuapp.com/), 2005-02-17, imsa.edu, LaTeX2HTML version of the original LaTeX document (https://quantum-algorithms.herokuapp.com/299/paper.tex), also available as PDF (https://quantum-algorithms.herokuapp.com/299/paper.pdf) or postscript (https://quantum-algorithms.herokuapp.com/299/paper.ps) document.
- Quantum Computation and Shor's Factoring Algorithm (http://homepages.cwi.nl/~rdewolf/publ/qc/survey.ps), Ronald de Wolf, CWI and University of Amsterdam, January 12, 1999, 9 page postscript document.
- Shor's Factoring Algorithm (http://www.cs.berkeley.edu/~vazirani/f04quantum/notes/lec9.ps), Notes from Lecture 9 of Berkeley CS 294–2, dated 4 Oct 2004, 7 page postscript document.
- Chapter 6 Quantum Computation (http://www.theory.caltech.edu/people/preskill/ph229/notes/chap6.ps) Archived (https://web.archive.org/web/20200430110523/http://www.theory.caltech.edu/people/preskill/ph229/notes/chap6.ps) 2020-04-30 at the Wayback Machine, 91 page postscript document, Caltech, Preskill, PH229.
- Quantum computation: a tutorial (http://www-users.cs.york.ac.uk/~schmuel/comp/comp.html) by Samuel L. Braunstein (http://www.cs.york.ac.uk/~schmuel/).
- The Quantum States of Shor's Algorithm (http://www.cs.ucr.edu/~neal/1996/cosc185-S96/shor/high-level.html), by Neal Young, Last modified: Tue May 21 11:47:38 1996.
- III. Breaking RSA Encryption with a Quantum Computer: Shor's Factoring Algorithm (https://web.archive.org/web/20121115112940/http://people.ccmr.cornell.edu/~mermin/qcomp/chap3.pdf), Lecture notes on Quantum computation, Cornell University, Physics 481–681, CS 483; Spring, 2006 by N. David Mermin. Last revised 2006-03-28, 30 page PDF document.
- Lavor, C.; Manssur, L. R. U.; Portugal, R. (2003). "Shor's Algorithm for Factoring Large Integers". arXiv:quant-ph/0303175 (https://arxiv.org/abs/quant-ph/0303175).
- Lomonaco, Jr (2000). "Shor's Quantum Factoring Algorithm". arXiv:quant-ph/0010034 (https://arxiv.org/abs/quant-ph/0010034). This paper is a written version of a one-hour lecture given on Peter Shor's quantum factoring algorithm. 22 pages.
- Chapter 20 Quantum Computation (http://www.cs.princeton.edu/theory/complexity/quantumchap.pdf), from *Computational Complexity: A Modern Approach*, Draft of a book: Dated January 2007, Sanjeev Arora and Boaz Barak, Princeton University. Published as Chapter 10 Quantum Computation of Sanjeev Arora, Boaz Barak, "Computational Complexity: A Modern Approach", Cambridge University Press, 2009, ISBN 978-0-521-42426-4
- A Step Toward Quantum Computing: Entangling 10 Billion Particles (http://blogs.discovermagazine.com/80beats/2011/01/19/a-step-towards-quantum-computing-entangling-10-billion-particles/) Archived (https://web.archive.org/web/20110120103006/http://blogs.discovermagazine.com/80beats/2011/01/19/a-step-towards-quantum-computing-entangling-10-billion-particles/) 2011-01-20 at the Wayback Machine, from "Discover Magazine", Dated January 19, 2011.
- Josef Gruska - *Quantum Computing Challenges* (http://www.fi.muni.cz/usr/gruska/survey1.ps) also in Mathematics unlimited: 2001 and beyond (https://www.amazon.com/Mathematics-Unlimited-Bj%C3%B6rn-Engquist/dp/3540669132), Editors Björn Engquist, Wilfried Schmid, Springer, 2001, ISBN 978-3-540-66913-5

External links

- Version 1.0.0 of libquantum (http://www.libquantum.de/): contains a C language implementation of Shor's algorithm with their simulated quantum computer library, but the width variable in shor.c should be set to 1 to improve the runtime complexity.
- PBS Infinite Series created two videos explaining the math behind Shor's algorithm, "How to Break Cryptography (http://www.pbs.org/video/how-to-break-cryptography-ahby1s/)" and "Hacking at Quantum Speed with Shor's Algorithm (http://www.pbs.org/video/hacking-at-quantum-speed-with-shors-algorithm-8jrjkq/)".
- Complete implementation of Shor's algorithm with Classiq (https://short.classiq.io/shor)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Shor%27s_algorithm&oldid=1245427578"

WIKIPEDIA
The Free Encyclopedia

Simon's problem

In computational complexity theory and quantum computing, **Simon's problem** is a computational problem that is proven to be solved exponentially faster on a quantum computer than on a classical (that is, traditional) computer. The quantum algorithm solving Simon's problem, usually called **Simon's algorithm**, served as the inspiration for Shor's algorithm.[1] Both problems are special cases of the abelian hidden subgroup problem, which is now known to have efficient quantum algorithms.

The problem is set in the model of decision tree complexity or query complexity and was conceived by Daniel R. Simon in 1994.[2] Simon exhibited a quantum algorithm that solves Simon's problem exponentially faster with exponentially fewer queries than the best probabilistic (or deterministic) classical algorithm. In particular, Simon's algorithm uses a linear number of queries and any classical probabilistic algorithm must use an exponential number of queries.

This problem yields an oracle separation between the complexity classes BPP (bounded-error classical query complexity) and BQP (bounded-error quantum query complexity).[3] This is the same separation that the Bernstein–Vazirani algorithm achieves, and different from the separation provided by the Deutsch–Jozsa algorithm, which separates P and EQP. Unlike the Bernstein–Vazirani algorithm, Simon's algorithm's separation is *exponential*.

Because this problem assumes the existence of a highly-structured "black box" oracle to achieve its speedup, this problem has little practical value.[4] However, without such an oracle, exponential speedups cannot easily be proven, since this would prove that P is different from PSPACE.

Problem description

Given a function (implemented by a black box or oracle) $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that, for some unknown $s \in \{0,1\}^n$, for all $x, y \in \{0,1\}^n$,

$$f(x) = f(y) \text{ if and only if } x \oplus y \in \{0^n, s\},$$

where $\oplus$ denotes bitwise XOR. The goal is to identify s by making as few queries to $f(x)$ as possible. Note that

$$a \oplus b = 0^n \text{ if and only if } a = b$$

Furthermore, for some x and s in $x \oplus y = s$, y is unique (not equal to x) if and only if $s \neq 0^n$. This means that f is two-to-one when $s \neq 0^n$, and one-to-one when $s = 0^n$. It is also the case that $x \oplus y = s$ implies $y = s \oplus x$, meaning that

$$f(x) = f(y) = f(x \oplus s)$$

which shows how f is periodic.

The associated decision problem formulation of Simon's problem is to distinguish when $s = 0^n$ (f is one-to-one), and when $s \neq 0^n$ (f is two-to-one).

Example

The following function is an example of a function that satisfies the required property for $n = 3$:

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

In this case, $s = 110$ (i.e. the solution). Every output of f occurs twice, and the two input strings corresponding to any one given output have bitwise XOR equal to $s = 110$.

For example, the input strings 010 and 100 are both mapped (by f) to the same output string 000. That is, $f(010) = 000$ and $f(100) = 000$. Applying XOR to 010 and 100 obtains 110, that is $010 \oplus 100 = 110 = s$.

$s = 110$ can also be verified using input strings 001 and 111 that are both mapped (by f) to the same output string 010. Applying XOR to 001 and 111 obtains 110, that is $001 \oplus 111 = 110 = s$. This gives the same solution $s = 110$ as before.

In this example the function *f* is indeed a two-to-one function where $s \neq 0^n$.

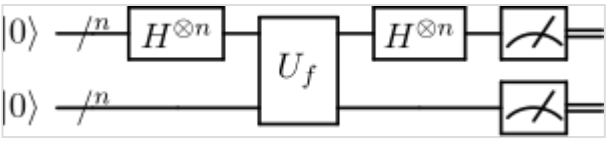
Problem hardness

Intuitively, this is a hard problem to solve in a "classical" way, even if one uses randomness and accepts a small probability of error. The intuition behind the hardness is reasonably simple: if you want to solve the problem classically, you need to find two different inputs x and y for which $f(x) = f(y)$. There is not necessarily any structure in the function f that would help us to find two such inputs: more specifically, we can discover something about f (or what it does) only when, for two different inputs, we obtain the same output. In any case, we would need to guess $\Omega(\sqrt{2^n})$ different inputs before being likely to find a pair on which f takes the same output, as per the birthday problem. Since, classically to find *s* with a 100% certainty it would require checking $\Theta(\sqrt{2^n})$ inputs, Simon's problem seeks to find *s* using fewer queries than this classical method.

Simon's algorithm

The algorithm as a whole uses a subroutine to execute the following two steps:

1. Run the quantum subroutine an expected $O(n)$ times to get a list of linearly independent bitstrings $y_1, \ldots, y_{n-1}$.
2. Each y_k satisfies $y_k \cdot s = 0$, so we can solve the system of equations this produces to get s.



Quantum circuit representing/implementing Simon's algorithm

Quantum subroutine

The quantum circuit (see the picture) is the implementation of the quantum part of Simon's algorithm. The quantum subroutine of the algorithm makes use of the Hadamard transform

$$H^{\otimes n}|k\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{k \cdot j} |j\rangle$$

where $k \cdot j = k_1 j_1 \oplus \ldots \oplus k_n j_n$, where $\oplus$ denotes XOR.

First, the algorithm starts with two registers, initialized to $|0\rangle^{\otimes n} |0\rangle^{\otimes n}$. Then, we apply the Hadamard transform to the first register, which gives the state

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle |0\rangle^{\otimes n}.$$

Query the oracle U_f to get the state

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle |f(k)\rangle.$$

Apply another Hadamard transform to the first register. This will produce the state

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{j \cdot k} |j\rangle \right] |f(k)\rangle = \sum_{j=0}^{2^n-1} |j\rangle \left[\frac{1}{2^n} \sum_{k=0}^{2^n-1} (-1)^{j \cdot k} |f(k)\rangle \right].$$

Finally, we measure the first register (the algorithm also works if the second register is measured before the first, but this is unnecessary). The probability of measuring a state $|j\rangle$ is

$$\left\| \frac{1}{2^n} \sum_{k=0}^{2^n-1} (-1)^{j \cdot k} |f(k)\rangle \right\|^2$$

This is due to the fact that taking the magnitude of this vector and squaring it sums up all the probabilities of all the possible measurements of the second register that must have the first register as $|j\rangle$. There are two cases for our measurement:

1. $s = 0^n$ and f is one-to-one.
2. $s \neq 0^n$ and f is two-to-one.

For the first case,

$$\left\| \frac{1}{2^n} \sum_{k=0}^{2^n-1} (-1)^{j \cdot k} |f(k)\rangle \right\|^2 = \frac{1}{2^n}$$

since in this case, f is one-to-one, implying that the range of f is $\{0,1\}^n$, meaning that the summation is over every basis vector. For the second case, note that there exist two strings, x_1 and x_2, such that $f(x_1) = f(x_2) = z$, where $z \in \mathbf{range}(f)$. Thus,

$$\left\| \frac{1}{2^n} \sum_{k=0}^{2^n-1} (-1)^{j \cdot k} |f(k)\rangle \right\|^2 = \left\| \frac{1}{2^n} \sum_{z \in \mathbf{range}(f)} ((-1)^{j \cdot x_1} + (-1)^{j \cdot x_2}) |z\rangle \right\|^2$$

Furthermore, since $x_1 \oplus x_2 = s$, $x_2 = x_1 \oplus s$, and so

$$\begin{aligned} \left\| \frac{1}{2^n} \sum_{z \in \mathbf{range}(f)} ((-1)^{j \cdot x_1} + (-1)^{j \cdot x_2}) |z\rangle \right\|^2 &= \left\| \frac{1}{2^n} \sum_{z \in \mathbf{range}(f)} ((-1)^{j \cdot x_1} + (-1)^{j \cdot (x_1 \oplus s)}) |z\rangle \right\|^2 \\ &= \left\| \frac{1}{2^n} \sum_{z \in \mathbf{range}(f)} ((-1)^{j \cdot x_1} + (-1)^{j \cdot x_1 \oplus j \cdot s}) |z\rangle \right\|^2 \\ &= \left\| \frac{1}{2^n} \sum_{z \in \mathbf{range}(f)} (-1)^{j \cdot x_1} (1 + (-1)^{j \cdot s}) |z\rangle \right\|^2 \end{aligned}$$

This expression is now easy to evaluate. Recall that we are measuring j. When $j \cdot s = 1$, then this expression will evaluate to 0, and when $j \cdot s = 0$, then this expression will be 2^{-n+1}.

Thus, both when $s = 0^n$ and when $s \neq 0^n$, our measured j satisfies $j \cdot s = 0$.

Classical post-processing

We run the quantum part of the algorithm until we have a linearly independent list of bitstrings $y_1, \ldots, y_{n-1}$, and each y_k satisfies $y_k \cdot s = 0$. Thus, we can efficiently solve this system of equations classically to find s.

The probability that $y_1, y_2, \ldots, y_{n-1}$ are linearly independent is at least

$$\prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) = 0.288788\ldots$$

Once we solve the system of equations, and produce a solution s', we can test if $f(0^n) = f(s')$. If this is true, then we know $s' = s$, since $f(0^n) = f(0^n \oplus s) = f(s)$. If it is the case that $f(0^n) \neq f(s')$, then that means that $s = 0^n$, and $f(0^n) \neq f(s')$ since f is one-to-one.

We can repeat Simon's algorithm a constant number of times to increase the probability of success arbitrarily, while still having the same time complexity.

Explicit examples of Simon's algorithm for few qubits

One qubit

Consider the simplest instance of the algorithm, with $n = 1$. In this case evolving the input state through an Hadamard gate and the oracle results in the state (up to renormalization):

$$|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle.$$

If $s = 1$, that is, $f(0) = f(1)$, then measuring the second register always gives the outcome $|f(0)\rangle$, and always results in the first register collapsing to the state (up to renormalization):

$$|0\rangle + |1\rangle.$$

Thus applying an Hadamard and measuring the first register always gives the outcome $|0\rangle$. On the other hand, if f is one-to-one, that is, $s = 0$, then measuring the first register after the second Hadamard can result in both $|0\rangle$ and $|1\rangle$, with equal probability.

We recover s from the measurement outcomes by looking at whether we measured always $|0\rangle$, in which case $s = 1$, or we measured both $|0\rangle$ and $|1\rangle$ with equal probability, in which case we infer that $s = 0$. This scheme will fail if $s = 0$ but we nonetheless always found the outcome $|0\rangle$, but the probability of this event is 2^{-N} with N the number of performed measurements, and can thus be made exponentially small by increasing the statistics.

Two qubits

Consider now the case with $n = 2$. The initial part of the algorithm results in the state (up to renormalization):

$$|00\rangle|f(00)\rangle + |01\rangle|f(01)\rangle + |10\rangle|f(10)\rangle + |11\rangle|f(11)\rangle.$$

If $s = (00)$, meaning f is injective, then finding $|f(x)\rangle$ on the second register always collapses the first register to $|x\rangle$, for all $x \in \{0,1\}^2$. In other words, applying Hadamard gates and measuring the first register the four outcomes $00, 01, 10, 11$ are thus found with equal probability.

Suppose on the other hand $s \neq (00)$, for example, $s = (01)$. Then measuring $|f(00)\rangle$ on the second register collapses the first register to the state $|00\rangle + |10\rangle$. And more generally, measuring $|f(xy)\rangle$ gives $|x, y\rangle + |x, y \oplus 1\rangle = |x\rangle(|0\rangle + |1\rangle)$ on the first register. Applying Hadamard gates and measuring on the first register can thus result in the outcomes 00 and 10 with equal probabilities.

Similar reasoning applies to the other cases: if $s = (10)$ then the possible outcomes are 00 and 01, while if $s = (11)$ the possible outcomes are 00 and 11, compatibly with the $j \cdot s = 0$ rule discussed in the general case.

To recover s we thus only need to distinguish between these four cases, collecting enough statistics to ensure that the probability of mistaking one outcome probability distribution for another is sufficiently small.

Complexity

Simon's algorithm requires $O(n)$ queries to the black box, whereas a classical algorithm would need at least $\Omega(2^{n/2})$ queries. It is also known that Simon's algorithm is optimal in the sense that *any* quantum algorithm to solve this problem requires $\Omega(n)$ queries.[5][6]

See also

- Deutsch–Jozsa algorithm

References

1. Shor, Peter W. (1999-01-01). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" (https://epubs.siam.org/doi/10.1137/S0036144598347011). *SIAM Review*. **41** (2): 303–332. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). doi:10.1137/S0036144598347011 (https://doi.org/10.1137%2FS0036144598347011). ISSN 0036-1445 (https://search.worldcat.org/issn/0036-1445).
2. Simon, Daniel R. (1997-10-01). "On the Power of Quantum Computation" (https://epubs.siam.org/doi/10.1137/S0097539796298637). *SIAM Journal on Computing*. **26** (5): 1474–1483. doi:10.1137/S0097539796298637 (https://doi.org/10.1137%2FS0097539796298637). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397).
3. Preskill, John (1998). *Lecture Notes for Physics 229: Quantum Information and Computation* (http://theory.caltech.edu/~preskill/ph229/). pp. 273–275.
4. Aaronson, Scott (2018). *Introduction to Quantum Information Science Lecture Notes* (https://www.scottaaronson.com/qclec.pdf) (PDF). pp. 144–151.
5. Koiran, P.; Nesme, V.; Portier, N. (2007), "The quantum query complexity of the Abelian hidden subgroup problem" (http://perso.ens-lyon.fr/pascal.koiran/Publis/lip.05-17.ps), *Theoretical Computer Science*, **380** (1–2): 115–126, doi:10.1016/j.tcs.2007.02.057 (https://doi.org/10.1016%2Fj.tcs.2007.02.057), retrieved 2011-06-06
6. Koiran, P.; Nesme, V.; Portier, N. (2005), "A quantum lower bound for the query complexity of Simon's Problem" (http://perso.ens-lyon.fr/pascal.koiran/Publis/icalp05.ps), *Proc. ICALP*, **3580**: 1287–1298, arXiv:quant-ph/0501060 (https://arxiv.org/abs/quant-ph/0501060), Bibcode:2005quant.ph..1060K (https://ui.adsabs.harvard.edu/abs/2005quant.ph..1060K), retrieved 2011-06-06

Retrieved from "https://en.wikipedia.org/w/index.php?title=Simon%27s_problem&oldid=1229697296"

WIKIPEDIA
The Free Encyclopedia

Variational quantum eigensolver

In quantum computing, the **variational quantum eigensolver** (**VQE**) is a quantum algorithm for quantum chemistry, quantum simulations and optimization problems. It is a hybrid algorithm that uses both classical computers and quantum computers to find the ground state of a given physical system. Given a guess or ansatz, the quantum processor calculates the expectation value of the system with respect to an observable, often the Hamiltonian, and a classical optimizer is used to improve the guess. The algorithm is based on the variational method of quantum mechanics.

It was originally proposed in 2014, with corresponding authors Alberto Peruzzo, Alán Aspuru-Guzik and Jeremy O'Brien.[a][1][2] The algorithm has also found applications in quantum machine learning and has been further substantiated by general hybrid algorithms between quantum and classical computers.[3] It is an example of a noisy intermediate-scale quantum (NISQ) algorithm.

Description

Pauli encoding

The objective of the VQE is to find a set of quantum operations that prepares the lowest energy state (or minima) of a close approximation to some target quantity or observable. While the only strict requirement for the representation of an observable is that it is efficient to estimate its expectation values, it is often simplest if that operator has a compact or simple expression in terms of Pauli operators or tensor products of Pauli operators.

For a fermionic system, it is often most convenient to qubitize: that is to write the many-body Hamiltonian of the system using second quantization, and then use a mapping to write the creation-annihiliation operators in terms of Pauli operators. Common schemes for fermions include Jordan–Wigner transformation, Bravyi-Kitaev transformation, and parity transformation.[4][5]

Once the Hamiltonian $\hat{H}$ is written in terms of Pauli operators and irrelevant states are discarded (finite-dimensional space), it would consist of a linear combination of Pauli strings $\hat{P}_i$ consisting of tensor products of Pauli operators (for example $X \otimes I \otimes Z \otimes X$), such that

$$\hat{H} = \sum_i \alpha_i \hat{P}_i,$$

where α_i are numerical coefficients. Based on the coefficients, the number of Pauli strings can be reduced in order to optimize the calculation.[6]

The VQE can be adapted to other optimization problems by adapting the Hamiltonian to be a cost function.[7]

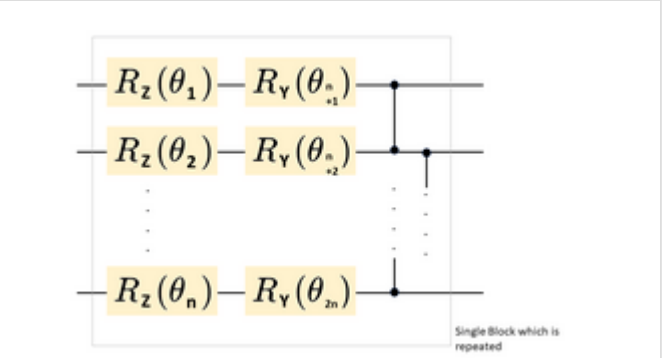
Ansatz and initial trial function

The choice of ansatz state depends on the system of interest. In gate-based quantum computing, the ansatz is given by a parametrized quantum circuit, whose parameters can be updated after each run. The ansatz has to be adaptable enough to not miss the desired state. A common method to obtain a valid ansatz is given by the unitary coupled cluster (UCC) framework and its extensions.[8]

If the ansatz is not chosen adequately the procedure may halt at suboptimal parameters that do not correspond to a minima. In this situation, the algorithm is said to have reached a 'barren plateau'.[5]

The ansatz can be set to an initial trial function to start the algorithm. For example, for a molecular system, one can use the Hartree–Fock method to provide a starting state that is close to the real ground state.

Another variant of the ansatz circuit is the hardware efficient ansatz, which consists of sequence of 1 qubit rotational gates and 2 qubit entangling gates. The number of repetitions of 1-qubit rotational gates and 2-qubit entangling gates is called the depth of the circuit.



Example of a hardware efficient ansatz.

Measurement

The expectation value of a given state $|\psi(\theta_1, \cdots, \theta_N)\rangle$ with parameters $\{\theta_i\}_{i=1}^N$, has an expectation value of the energy or cost function given by

$$E(\theta_1, \cdots, \theta_n) = \langle \hat{H} \rangle = \sum_i \alpha_i \langle \psi(\theta_1, \cdots, \theta_N) | \hat{P}_i | \psi(\theta_1, \cdots, \theta_N) \rangle$$

so in order to obtain the expectation value of the energy, one can measure the expectation value of each Pauli string (number of counts for a given value over the total number of counts). This step corresponds to measuring each qubit in the axis provided by the Pauli string.[7] For example, for the string $X \otimes Y \otimes Y$, the first qubit is to be measured in the *x*-axis, while the last two are to be measured in the *y*-axis of the Bloch sphere. If measurement in the *z*-axis is only possible, then Clifford gates can be used to transform between axes. If two Pauli strings commute, then they can be both measured simultaneously using the same circuit and interpreting the result according to the Pauli algebra.

Variational method and optimization

Given a parametrized ansatz for the ground state eigenstate, with parameters that can be modified, one is sure to find the parametrized state that is closest to the ground state based on the variational method of quantum mechanics. Using classical algorithms in a digital computer, the parameters of the ansatz can be

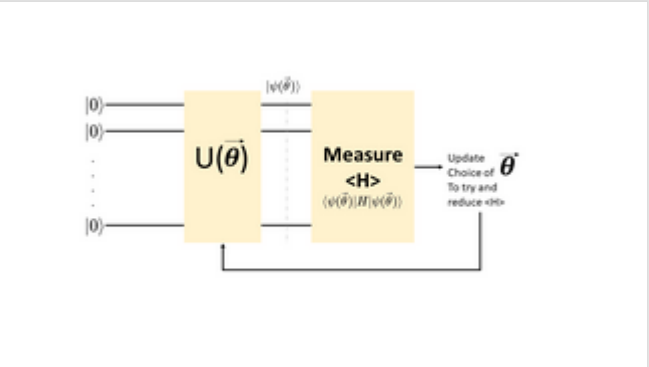
optimized. For this minimization, it is necessary to find the minima of a multivariable function. Classical optimizers using gradient descent can be used for this purpose.[7]

Formulation

For a given Hamiltonian (H) and a state vector $|\psi\rangle$ if we can vary $|\psi\rangle$ arbitrarily then $\min_{|\psi\rangle}\langle\psi|H|\psi\rangle$ will be the ground state energy and $\operatorname{argmin}_{|\psi\rangle}\langle\psi|H|\psi\rangle$ would be a ground state (assuming no degeneracy). But the above minimization problem over all possible states $|\psi\rangle$, where state $|\psi\rangle$ is 2^n dimensional, is impractical. Thus to restrict the search space to a more practical size (eg. poly(n)), we need to restrict the $|\psi\rangle$ to only a subset of possible n-qubit states which is based on conventional physics, chemistry and quantum mechanics knowledge.

Algorithm

The adjoining figure illustrates the high level steps in the VQE algorithm.



High Level illustration of Variational Quantum Algorithm

The circuit $U(\vec{\theta})$ controls the subset of possible states that can be created, and the parameter $\vec{\theta}$ contains the variational parameters, $\vec{\theta} = \begin{pmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_p \end{pmatrix}$ where the number of parameters chosen are enough to lend the algorithm expressive power to compute the ground state of the system, but not too big to increase the computational cost of the optimization step.

By running the circuit many times and constantly updating the parameters to find the global minima of the expectation value of the desired observable, one can approach the ground state of the given system and store it in a quantum processor as a series of quantum gate instructions.

In case of gradient descent, its required to minimize a cost function $f(\vec{\theta})$ where for the VQE case $f(\vec{\theta}) = \langle\psi(\vec{\theta})|H|\psi(\vec{\theta})\rangle$. The update rule is:

$$\vec{\theta}^{(\text{new})} = \vec{\theta}^{(\text{old})} - r\nabla f(\vec{\theta}^{(\text{old})})$$

where *r* is the learning rate (step size) and

$$\Delta f(\vec{\theta}^{(\text{old})}) = \left(\frac{\partial f(\vec{\theta}^{(\text{old})})}{\partial\theta_1}, \frac{\partial f(\vec{\theta}^{(\text{old})})}{\partial\theta_2}, \dots\right)^\top$$

In order to compute the gradients, the parameter shift rule is used.

Example

Considering a single Pauli gate example:

$$U(\theta) = e^{-i\frac{\theta}{2}P},$$

where *P = X,Y or Z*, then

$$\nabla_\theta U = \frac{\partial U}{\partial \theta} = -\frac{i}{2}Pe^{-i\frac{\theta}{2}P} = -\frac{i}{2}PU = -\frac{i}{2}UP$$

As, $f(\theta) = \langle\phi|U^\dagger AU|\phi\rangle$. Thus,

$$\nabla_\theta f(\theta) = \frac{\partial}{\partial\theta}\langle\phi|U^\dagger AU|\phi\rangle = \langle\phi|\left(\frac{i}{2}P\right)U^\dagger AU|\phi\rangle + \langle\phi|U^\dagger A\left(-\frac{i}{2}P\right)U|\phi\rangle$$

$$= \frac{1}{2}\langle\phi|U^\dagger(\theta+\frac{\pi}{2})AU(\theta+\frac{\pi}{2})|\phi\rangle - \frac{1}{2}\langle\phi|U^\dagger(\theta-\frac{\pi}{2})AU(\theta-\frac{\pi}{2})|\phi\rangle$$

$$= \frac{1}{2}\left(f(\theta+\frac{\pi}{2}) - f(\theta-\frac{\pi}{2})\right)$$

The above result has interesting properties as:

1. The same circuit can be used to evaluate $f(\theta)$ and $\nabla_\theta f(\theta)$
2. $f(\cdot)$ needs to be evaluated 2 times to arrive at the gradient value
3. As the angle precision $\pm\frac{\pi}{2}$ is large, gate precision can be kept low

Advantages and disadvantages

1. The VQE circuit does not require many gates compared with quantum phase estimation algorithm (QPE), it is more robust to errors and lends itself well to error mitigation strategies.
2. Its a heuristic method and thus does not guarantee convergence to the ground state value. The method is highly influenced by the choice of ansatz circuit and the optimization methods.
3. Number of measurements required to conclude the value of ground state is higher compared to the QPE and scales approximately with the number of terms in the Hamiltonian.
4. VQE can run on NISQ hardware.
5. VQE is highly versatile, as problems (apart from chemistry) can be expressed as Hamiltonians.

Use

In chemistry

As of 2022, the variational quantum eigensolver can only simulate small molecules like the helium hydride ion[1] or the beryllium hydride molecule.[9] Larger molecules can be simulated by taking into account symmetry considerations. In 2020, a 12-qubit simulation of a hydrogen chain (H_{12}) was demonstrated using Google's Sycamore quantum processor.[10]

See also

- Quantum optimization algorithms

Notes

a. Full authors: Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alan Aspuru-Guzik and Jeremy L. O'Brien. All equally contributing.

References

1. Peruzzo, Alberto; McClean, Jarrod; Shadbolt, Peter; Yung, Man-Hong; Zhou, Xiao-Qi; Love, Peter J.; Aspuru-Guzik, Alán; O'Brien, Jeremy L. (2014). "A variational eigenvalue solver on a photonic quantum processor" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4124861). *Nature Communications*. **5** (1): 4213. arXiv:1304.3061 (https://arxiv.org/abs/1304.3061). Bibcode:2014NatCo...5.4213P (https://ui.adsabs.harvard.edu/abs/2014NatCo...5.4213P). doi:10.1038/ncomms5213 (https://doi.org/10.1038%2Fncomms5213). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 4124861 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4124861). PMID 25055053 (https://pubmed.ncbi.nlm.nih.gov/25055053).
2. Bharti, Kishor; Cervera-Lierta, Alba; Kyaw, Thi Ha; Haug, Tobias; Alperin-Lea, Sumner; Anand, Abhinav; Degroote, Matthias; Heimonen, Hermanni; Kottmann, Jakob S.; Menke, Tim; Mok, Wai-Keong; Sim, Sukin; Kwek, Leong-Chuan; Aspuru-Guzik, Alán (2022-02-15). "Noisy intermediate-scale quantum algorithms" (https://link.aps.org/doi/10.1103/RevModPhys.94.015004). *Reviews of Modern Physics*. **94** (1): 015004. arXiv:2101.08448 (https://arxiv.org/abs/2101.08448). Bibcode:2022RvMP...94a5004B (https://ui.adsabs.harvard.edu/abs/2022RvMP...94a5004B). doi:10.1103/RevModPhys.94.015004 (https://doi.org/10.1103%2FRevModPhys.94.015004). hdl:10356/161272 (https://hdl.handle.net/10356%2F161272).
3. McClean, Jarrod R; Romero, Jonathan; Babbush, Ryan; Aspuru-Guzik, Alán (2016-02-04). "The theory of variational hybrid quantum-classical algorithms" (https://doi.org/10.1088%2F1367-2630%2F18%2F2%2F023023). *New Journal of Physics*. **18** (2): 023023. arXiv:1509.04279 (https://arxiv.org/abs/1509.04279). Bibcode:2016NJPh...18b3023M (https://ui.adsabs.harvard.edu/abs/2016NJPh...18b3023M). doi:10.1088/1367-2630/18/2/023023 (https://doi.org/10.1088%2F1367-2630%2F18%2F2%2F023023). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 92988541 (https://api.semanticscholar.org/CorpusID:92988541).
4. Steudtner, M (2019). *Methods to simulate fermions on quantum computers with hardware limitations* (https://scholarlypublications.universiteitleiden.nl/handle/1887/80413) (PhD Thesis). University of Leiden.
5. Tilly, Jules; Chen, Hongxiang; Cao, Shuxiang; Picozzi, Dario; Setia, Kanav; Li, Ying; Grant, Edward; Wossnig, Leonard; Rungger, Ivan; Booth, George H.; Tennyson, Jonathan (2022-06-12). "The Variational Quantum Eigensolver: A review of methods and best practices". *Physics Reports*. **986**: 1–128. arXiv:2111.05176 (https://arxiv.org/abs/2111.05176). Bibcode:2022PhR...986....1T (https://ui.adsabs.harvard.edu/abs/2022PhR...986....1T).

doi:10.1016/j.physrep.2022.08.003 (https://doi.org/10.1016%2Fj.physrep.2022.08.003). S2CID 243861087 (https://api.semanticscholar.org/CorpusID:243861087).

6. Seeley, Jacob T.; Richard, Martin J.; Love, Peter J. (2012-12-12). "The Bravyi-Kitaev transformation for quantum computation of electronic structure" (https://aip.scitation.org/doi/abs/10.1063/1.4768229). *The Journal of Chemical Physics*. **137** (22): 224109. arXiv:1208.5986 (https://arxiv.org/abs/1208.5986). Bibcode:2012JChPh.137v4109S (https://ui.adsabs.harvard.edu/abs/2012JChPh.137v4109S). doi:10.1063/1.4768229 (https://doi.org/10.1063%2F1.4768229). ISSN 0021-9606 (https://search.worldcat.org/issn/0021-9606). PMID 23248989 (https://pubmed.ncbi.nlm.nih.gov/23248989). S2CID 30699239 (https://api.semanticscholar.org/CorpusID:30699239).
7. Moll, Nikolaj; Barkoutsos, Panagiotis; Bishop, Lev S; Chow, Jerry M; Cross, Andrew; Egger, Daniel J; Filipp, Stefan; Fuhrer, Andreas; Gambetta, Jay M; Ganzhorn, Marc; Kandala, Abhinav; Mezzacapo, Antonio; Müller, Peter; Riess, Walter; Salis, Gian (2018). "Quantum optimization using variational algorithms on near-term quantum devices" (https://iopscience.iop.org/article/10.1088/2058-9565/aab822). *Quantum Science and Technology*. **3** (3): 030503. arXiv:1710.01022 (https://arxiv.org/abs/1710.01022). Bibcode:2018QS&T....3c0503M (https://ui.adsabs.harvard.edu/abs/2018QS&T....3c0503M). doi:10.1088/2058-9565/aab822 (https://doi.org/10.1088%2F2058-9565%2Faab822). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 56376912 (https://api.semanticscholar.org/CorpusID:56376912).
8. Tilly, Jules; Chen, Hongxiang; Cao, Shuxiang; Picozzi, Dario; Setia, Kanav; Li, Ying; Grant, Edward; Wossnig, Leonard; Rungger, Ivan; Booth, George H.; Tennyson, Jonathan (2022-06-12). "The Variational Quantum Eigensolver: A review of methods and best practices". *Physics Reports*. **986**: 1–128. arXiv:2111.05176 (https://arxiv.org/abs/2111.05176). Bibcode:2022PhR...986....1T (https://ui.adsabs.harvard.edu/abs/2022PhR...986....1T). doi:10.1016/j.physrep.2022.08.003 (https://doi.org/10.1016%2Fj.physrep.2022.08.003). S2CID 243861087 (https://api.semanticscholar.org/CorpusID:243861087).
9. Kandala, Abhinav; Mezzacapo, Antonio; Temme, Kristan; Takita, Maika; Brink, Markus; Chow, Jerry M.; Gambetta, Jay M. (2017). "Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets" (https://www.nature.com/articles/nature23879). *Nature*. **549** (7671): 242–246. arXiv:1704.05018 (https://arxiv.org/abs/1704.05018). Bibcode:2017Natur.549..242K (https://ui.adsabs.harvard.edu/abs/2017Natur.549..242K). doi:10.1038/nature23879 (https://doi.org/10.1038%2Fnature23879). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 28905916 (https://pubmed.ncbi.nlm.nih.gov/28905916). S2CID 4390182 (https://api.semanticscholar.org/CorpusID:4390182).
10. Arute, Frank; Arya, Kunal; Babbush, Ryan; et al. (2020). "Hartree-Fock on a superconducting qubit quantum computer" (https://www.science.org/doi/10.1126/science.abb9811). *Science*. **369** (6507): 1084–1089. arXiv:2004.04174 (https://arxiv.org/abs/2004.04174). Bibcode:2020Sci...369.1084. (https://ui.adsabs.harvard.edu/abs/2020Sci...369.1084.). doi:10.1126/science.abb9811 (https://doi.org/10.1126%2Fscience.abb9811). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 32855334 (https://pubmed.ncbi.nlm.nih.gov/32855334). S2CID 215548188 (https://api.semanticscholar.org/CorpusID:215548188).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Variational_quantum_eigensolver&oldid=1232323064"

WIKIPEDIA
The Free Encyclopedia

Quantum complexity theory

Quantum complexity theory is the subfield of computational complexity theory that deals with complexity classes defined using quantum computers, a computational model based on quantum mechanics. It studies the hardness of computational problems in relation to these complexity classes, as well as the relationship between quantum complexity classes and classical (i.e., non-quantum) complexity classes.

Two important quantum complexity classes are BQP and QMA.

Background

A complexity class is a collection of computational problems that can be solved by a computational model under certain resource constraints. For instance, the complexity class P is defined as the set of problems solvable by a Turing machine in polynomial time. Similarly, quantum complexity classes may be defined using quantum models of computation, such as the quantum circuit model or the equivalent quantum Turing machine. One of the main aims of quantum complexity theory is to find out how these classes relate to classical complexity classes such as P, NP, BPP, and PSPACE.

One of the reasons quantum complexity theory is studied are the implications of quantum computing for the modern Church-Turing thesis. In short the modern Church-Turing thesis states that any computational model can be simulated in polynomial time with a probabilistic Turing machine.[1][2] However, questions around the Church-Turing thesis arise in the context of quantum computing. It is unclear whether the Church-Turing thesis holds for the quantum computation model. There is much evidence that the thesis does not hold. It may not be possible for a probabilistic Turing machine to simulate quantum computation models in polynomial time.[1]

Both quantum computational complexity of functions and classical computational complexity of functions are often expressed with asymptotic notation. Some common forms of asymptotic notion of functions are $O(T(n))$, $\Omega(T(n))$, and $\Theta(T(n))$. $O(T(n))$ expresses that something is bounded above by $cT(n)$ where c is a constant such that $c > 0$ and $T(n)$ is a function of n, $\Omega(T(n))$ expresses that something is bounded below by $cT(n)$ where c is a constant such that $c > 0$ and $T(n)$ is a function of n, and $\Theta(T(n))$ expresses both $O(T(n))$ and $\Omega(T(n))$.[3] These notations also have their own names. $O(T(n))$ is called Big O notation, $\Omega(T(n))$ is called Big Omega notation, and $\Theta(T(n))$ is called Big Theta notation.

Overview of complexity classes

The important complexity classes P, BPP, BQP, PP, and PSPACE can be compared based on promise problems. A promise problem is a decision problem which has an input assumed to be selected from the set of all possible input strings. A promise problem is a pair $A = (A_{\text{yes}}, A_{\text{no}})$, where A_{yes} is the set of

yes instances and A_{no} is the set of no instances, and the intersection of these sets is empty: $A_{\text{yes}} \cap A_{\text{no}} = \varnothing$. All of the previous complexity classes contain promise problems.[4]

Complexity Class	Criteria
P	Promise problems for which a polynomial time deterministic Turing machine accepts all strings in A_{yes} and rejects all strings in A_{no}[4]
BPP	Promise problems for which a polynomial time Probabilistic Turing machine accepts every string in A_{yes} with a probability of at least $\frac{2}{3}$, and accepts every string in A_{no} with a probability of at most $\frac{1}{3}$[4]
BQP	Promise problems such that for functions $a, b : \mathbb{N} \to [0,1]$, there exists a polynomial time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where Q_n is a circuit which accepts n qubits and gives an output of one qubit. An element x of A_{yes} is accepted by Q with a probability greater than or equal to $a(\lvert x\rvert)$. An element x of A_{no} is accepted by Q with a probability less than or equal to $b(\lvert x\rvert)$.[4]
PP	Promise problems for which a polynomial time Probabilistic Turing machine accepts every string in A_{yes} with a probability greater than $\frac{1}{2}$, and accepts every string in A_{no} with a probability of at most $\frac{1}{2}$[4]
PSPACE	Promise problems for which a deterministic Turing machine, that runs in polynomial space, accepts every string in A_{yes} and rejects all strings in A_{no}[4]

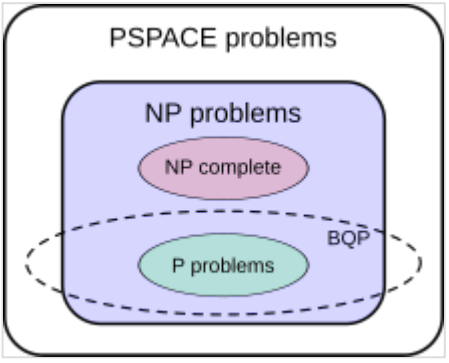
BQP

The class of problems that can be efficiently solved by a quantum computer with bounded error is called BQP ("bounded error, quantum, polynomial time"). More formally, BQP is the class of problems that can be solved by a polynomial-time quantum Turing machine with error probability of at most 1/3.

BQP algorithm (1 run)

Correct answer \ Answer produced	Yes	No
Yes	≥ 2/3	≤ 1/3
No	≤ 1/3	≥ 2/3

As a class of probabilistic problems, BQP is the quantum counterpart to BPP ("bounded error, probabilistic, polynomial time"), the class of problems that can be efficiently solved by probabilistic Turing machines with bounded error.[6] It is known that $\mathbf{BPP} \subseteq \mathbf{BQP}$ and widely suspected, but not proven, that $\mathbf{BQP} \nsubseteq \mathbf{BPP}$, which intuitively would mean that quantum computers are more powerful than classical computers in terms of time complexity.[7] BQP is a subset of PP.



The suspected relationship of BQP to other complexity classes[5]

The exact relationship of BQP to P, NP, and PSPACE is not known. However, it is known that $\mathbf{P} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE}$; that is, the class of problems that can be efficiently solved by quantum computers includes all problems that can be efficiently solved by deterministic classical computers but does not include any

problems that cannot be solved by classical computers with polynomial space resources. It is further suspected that BQP is a strict superset of P, meaning there are problems that are efficiently solvable by quantum computers that are not efficiently solvable by deterministic classical computers. For instance, integer factorization and the discrete logarithm problem are known to be in BQP and are suspected to be outside of P. On the relationship of BQP to NP, little is known beyond the fact that some NP problems are in BQP (integer factorization and the discrete logarithm problem are both in NP, for example). It is suspected that $\mathsf{NP} \not\subseteq \mathsf{BQP}$; that is, it is believed that there are efficiently checkable problems that are not efficiently solvable by a quantum computer. As a direct consequence of this belief, it is also suspected that BQP is disjoint from the class of NP-complete problems (if any NP-complete problem were in BQP, then it follows from NP-hardness that all problems in NP are in BQP).[8]

The relationship of BQP to the essential classical complexity classes can be summarized as:

$$\mathsf{P} \subseteq \mathsf{BPP} \subseteq \mathsf{BQP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE}$$

It is also known that BQP is contained in the complexity class $\#\mathsf{P}$ (or more precisely in the associated class of decision problems $\mathsf{P}^{\#\mathsf{P}}$),[8] which is a subset of PSPACE.

Simulation of quantum circuits

There is no known way to efficiently simulate a quantum computational model with a classical computer. This means that a classical computer cannot simulate a quantum computational model in polynomial time. However, a quantum circuit of $S(n)$ qubits with $T(n)$ quantum gates can be simulated by a classical circuit with $O(2^{S(n)}T(n)^3)$ classical gates.[3] This number of classical gates is obtained by determining how many bit operations are necessary to simulate the quantum circuit. In order to do this, first the amplitudes associated with the $S(n)$ qubits must be accounted for. Each of the states of the $S(n)$ qubits can be described by a two-dimensional complex vector, or a state vector. These state vectors can also be described a linear combination of its component vectors with coefficients called amplitudes. These amplitudes are complex numbers which are normalized to one, meaning the sum of the squares of the absolute values of the amplitudes must be one.[3] The entries of the state vector are these amplitudes. Which entry each of the amplitudes are correspond to the none-zero component of the component vector which they are the coefficients of in the linear combination description. As an equation this is described as $\alpha\begin{bmatrix}1\\0\end{bmatrix}+\beta\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ or $\alpha\left|1\right\rangle+\beta\left|0\right\rangle=\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ using Dirac notation. The state of the entire $S(n)$ qubit system can be described by a single state vector. This state vector describing the entire system is the tensor product of the state vectors describing the individual qubits in the system. The result of the tensor products of the $S(n)$ qubits is a single state vector which has $2^{S(n)}$ dimensions and entries that are the amplitudes associated with each basis state or component vector. Therefore, $2^{S(n)}$ amplitudes must be accounted for with a $2^{S(n)}$ dimensional complex vector which is the state vector for the $S(n)$ qubit system.[9] In order to obtain an upper bound for the number of gates required to simulate a quantum circuit we need a sufficient upper bound for the amount data used to specify the information about each of the $2^{S(n)}$ amplitudes. To do this $O(T(n))$ bits of precision are sufficient for encoding each amplitude.[3] So it takes $O(2^{S(n)}T(n))$ classical bits to account for the state vector of the $S(n)$ qubit system. Next the application of the $T(n)$ quantum gates on $2^{S(n)}$ amplitudes must be accounted for. The quantum gates can be represented as $2^{S(n)} \times 2^{S(n)}$ sparse matrices.[3] So to account for the application of

each of the $T(n)$ quantum gates, the state vector must be multiplied by a $2^{S(n)} \times 2^{S(n)}$ sparse matrix for each of the $T(n)$ quantum gates. Every time the state vector is multiplied by a $2^{S(n)} \times 2^{S(n)}$ sparse matrix, $O(2^{S(n)})$ arithmetic operations must be performed.[3] Therefore, there are $O(2^{S(n)}T(n)^2)$ bit operations for every quantum gate applied to the state vector. So $O(2^{S(n)}T(n)^2)$ classical gate are needed to simulate $S(n)$ qubit circuit with just one quantum gate. Therefore, $O(2^{S(n)}T(n)^3)$ classical gates are needed to simulate a quantum circuit of $S(n)$ qubits with $T(n)$ quantum gates.[3] While there is no known way to efficiently simulate a quantum computer with a classical computer, it is possible to efficiently simulate a classical computer with a quantum computer. This is evident from the fact that $\mathsf{BPP} \subseteq \mathsf{BQP}$.[4]

Quantum query complexity

One major advantage of using a quantum computational system instead of a classical one, is that a quantum computer may be able to give a polynomial time algorithm for some problem for which no classical polynomial time algorithm exists, but more importantly, a quantum computer may significantly decrease the calculation time for a problem that a classical computer can already solve efficiently. Essentially, a quantum computer may be able to both determine how long it will take to solve a problem, while a classical computer may be unable to do so, and can also greatly improve the computational efficiency associated with the solution to a particular problem. Quantum query complexity refers to how complex, or how many queries to the graph associated with the solution of a particular problem, are required to solve the problem. Before we delve further into query complexity, let us consider some background regarding graphing solutions to particular problems, and the queries associated with these solutions.

Query models of directed graphs

One type of problem that quantum computing can make easier to solve are graph problems. If we are to consider the amount of queries to a graph that are required to solve a given problem, let us first consider the most common types of graphs, called directed graphs, that are associated with this type of computational modelling. In brief, directed graphs are graphs where all edges between vertices are unidirectional. Directed graphs are formally defined as the graph $G = (N, E)$, where N is the set of vertices, or nodes, and E is the set of edges.[10]

Adjacency matrix model

When considering quantum computation of the solution to directed graph problems, there are two important query models to understand. First, there is the adjacency matrix model, where the graph of the solution is given by the adjacency matrix: $M \in \{0,1\}a^{n\mathrm{X}n}$, with $M_{ij} = 1$, if and only if $(v_i, v_j) \in E$.[11]

Adjacency array model

Next, there is the slightly more complicated adjacency array model built on the idea of adjacency lists, where every vertex, u, is associated with an array of neighboring vertices such that $f_i : [d_i^+] \to [n]$, for the out-degrees of vertices $d_i^+, \ldots, d_n^+$, where n is the minimum value of the upper bound of this model,

and $f_i(j)$ returns the "j^{th}" vertex adjacent to i. Additionally, the adjacency array model satisfies the simple graph condition, $\forall i \in [n], j, j' \in [k], j \neq j' : f_i(j) \neq f_i(j')$, meaning that there is only one edge between any pair of vertices, and the number of edges is minimized throughout the entire model (see Spanning tree model for more background).[11]

Quantum query complexity of certain types of graph problems

Both of the above models can be used to determine the query complexity of particular types of graphing problems, including the connectivity, strong connectivity (a directed graph version of the connectivity model), minimum spanning tree, and single source shortest path models of graphs. An important caveat to consider is that the quantum complexity of a particular type of graphing problem can change based on the query model (namely either matrix or array) used to determine the solution. The following table showing the quantum query complexities of these types of graphing problems illustrates this point well.

Quantum query complexity of certain types of graph problems

Problem	Matrix model	Array model
Minimum spanning tree	$\Theta(n^{3/2})$	$\Theta(\sqrt{nm})$
Connectivity	$\Theta(n^{3/2})$	$\Theta(n)$
Strong connectivity	$\Theta(n^{3/2})$	$\Omega(\sqrt{nm})$, $O(\sqrt{nm\log(n)})$
Single source shortest path	$\Omega(n^{3/2})$, $O(n^{3/2}\log^2 n)$	$\Omega(\sqrt{nm})$, $O(\sqrt{nm}\log^2(n))$

Notice the discrepancy between the quantum query complexities associated with a particular type of problem, depending on which query model was used to determine the complexity. For example, when the matrix model is used, the quantum complexity of the connectivity model in Big O notation is $\Theta(n^{3/2})$, but when the array model is used, the complexity is $\Theta(n)$. Additionally, for brevity, we use the shorthand m in certain cases, where $m = \Theta(n^2)$.[11] The important implication here is that the efficiency of the algorithm used to solve a graphing problem is dependent on the type of query model used to model the graph.

Other types of quantum computational queries

In the query complexity model, the input can also be given as an oracle (black box). The algorithm gets information about the input only by querying the oracle. The algorithm starts in some fixed quantum state and the state evolves as it queries the oracle.

Similar to the case of graphing problems, the quantum query complexity of a black-box problem is the smallest number of queries to the oracle that are required in order to calculate the function. This makes the quantum query complexity a lower bound on the overall time complexity of a function.

Grover's algorithm

An example depicting the power of quantum computing is Grover's algorithm for searching unstructured databases. The algorithm's quantum query complexity is $O(\sqrt{N})$, a quadratic improvement over the best possible classical query complexity $O(N)$, which is a linear search. Grover's algorithm is asymptotically

optimal; in fact, it uses at most a $1 + o(1)$ fraction more queries than the best possible algorithm.[12]

Deutsch-Jozsa algorithm

The Deutsch-Jozsa algorithm is a quantum algorithm designed to solve a toy problem with a smaller query complexity than is possible with a classical algorithm. The toy problem asks whether a function $f : \{0,1\}^n \to \{0,1\}$ is constant or balanced, those being the only two possibilities.[2] The only way to evaluate the function f is to consult a black box or oracle. A classical deterministic algorithm will have to check more than half of the possible inputs to be sure of whether or not the function is constant or balanced. With 2^n possible inputs, the query complexity of the most efficient classical deterministic algorithm is $2^{n-1} + 1$.[2] The Deutsch-Jozsa algorithm takes advantage of quantum parallelism to check all of the elements of the domain at once and only needs to query the oracle once, making its query complexity 1.[2]

Other theories of quantum physics

It has been speculated that further advances in physics could lead to even faster computers. For instance, it has been shown that a non-local hidden variable quantum computer based on Bohmian Mechanics could implement a search of an N-item database in at most $O(\sqrt[3]{N})$ steps, a slight speedup over Grover's algorithm, which runs in $O(\sqrt{N})$ steps. Note, however, that neither search method would allow quantum computers to solve NP-complete problems in polynomial time.[13] Theories of quantum gravity, such as M-theory and loop quantum gravity, may allow even faster computers to be built. However, defining computation in these theories is an open problem due to the problem of time; that is, within these physical theories there is currently no obvious way to describe what it means for an observer to submit input to a computer at one point in time and then receive output at a later point in time.[14][15]

See also

- Quantum computing
- Quantum Turing machine
- Polynomial hierarchy (PH)

Notes

1. Vazirani, Umesh V. (2002). "A survey of quantum complexity theory" (https://dx.doi.org/10.1090/psapm/058/1922899). *Proceedings of Symposia in Applied Mathematics*. **58**: 193–217. doi:10.1090/psapm/058/1922899 (https://doi.org/10.1090%2Fpsapm%2F058%2F1922899). ISBN 9780821820841. ISSN 2324-7088 (https://search.worldcat.org/issn/2324-7088).
2. Nielsen, Michael A., 1974- (2010). *Quantum computation and quantum information* (https://www.worldcat.org/oclc/665137861). Chuang, Isaac L., 1968- (10th anniversary ed.). Cambridge: Cambridge University Press. ISBN 978-1-107-00217-3. OCLC 665137861 (https://search.worldcat.org/oclc/665137861).

3. Cleve, Richard (2000), "An Introduction to Quantum Complexity Theory" (https://dx.doi.org/10.1142/9789810248185_0004), *Quantum Computation and Quantum Information Theory*, WORLD SCIENTIFIC, pp. 103–127, arXiv:quant-ph/9906111 (https://arxiv.org/abs/quant-ph/9906111), Bibcode:2000qcqi.book..103C (https://ui.adsabs.harvard.edu/abs/2000qcqi.book..103C), doi:10.1142/9789810248185_0004 (https://doi.org/10.1142%2F9789810248185_0004), ISBN 978-981-02-4117-9, S2CID 958695 (https://api.semanticscholar.org/CorpusID:958695), retrieved October 10, 2020
4. Watrous, John (2008-04-21). "Quantum Computational Complexity". arXiv:0804.3401 (https://arxiv.org/abs/0804.3401) [quant-ph (https://arxiv.org/archive/quant-ph)].
5. Nielsen, p. 42
6. Nielsen, Michael; Chuang, Isaac (2000). *Quantum Computation and Quantum Information* (https://books.google.com/books?id=aai-P4V9GJ8C). Cambridge: Cambridge University Press. p. 41. ISBN 978-0-521-63503-5. OCLC 174527496 (https://search.worldcat.org/oclc/174527496).
7. Nielsen, p. 201
8. Bernstein, Ethan; Vazirani, Umesh (1997). "Quantum Complexity Theory" (http://www.cs.berkeley.edu/~vazirani/bv.ps). *SIAM Journal on Computing*. **26** (5): 1411–1473. CiteSeerX 10.1.1.144.7852 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.7852). doi:10.1137/S0097539796300921 (https://doi.org/10.1137%2FS0097539796300921).
9. Häner, Thomas; Steiger, Damian S. (2017-11-12). "0.5 petabyte simulation of a 45-qubit quantum circuit" (https://dx.doi.org/10.1145/3126908.3126947). *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. New York, NY, USA: ACM. pp. 1–10. arXiv:1704.01127 (https://arxiv.org/abs/1704.01127). doi:10.1145/3126908.3126947 (https://doi.org/10.1145%2F3126908.3126947). ISBN 978-1-4503-5114-0. S2CID 3338733 (https://api.semanticscholar.org/CorpusID:3338733).
10. Nykamp, D.Q. "Directed Graph Definition" (https://mathinsight.org/definition/directed_graph).
11. Durr, Christoph; Heiligman, Mark; Hoyer, Peter; Mhalla, Mehdi (January 2006). "Quantum query complexity of some graph problems". *SIAM Journal on Computing*. **35** (6): 1310–1328. arXiv:quant-ph/0401091 (https://arxiv.org/abs/quant-ph/0401091). doi:10.1137/050644719 (https://doi.org/10.1137%2F050644719). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397). S2CID 27736397 (https://api.semanticscholar.org/CorpusID:27736397).
12. Zalka, Christof (1999-10-01). "Grover's quantum searching algorithm is optimal" (https://link.aps.org/doi/10.1103/PhysRevA.60.2746). *Physical Review A*. **60** (4): 2746–2751. arXiv:quant-ph/9711070 (https://arxiv.org/abs/quant-ph/9711070). Bibcode:1999PhRvA..60.2746Z (https://ui.adsabs.harvard.edu/abs/1999PhRvA..60.2746Z). doi:10.1103/PhysRevA.60.2746 (https://doi.org/10.1103%2FPhysRevA.60.2746). S2CID 1542077 (https://api.semanticscholar.org/CorpusID:1542077).
13. Aaronson, Scott. "Quantum Computing and Hidden Variables" (http://www.scottaaronson.com/papers/qchvpra.pdf) (PDF).
14. Aaronson, Scott (2005). "NP-complete Problems and Physical Reality". *ACM SIGACT News*. **2005**. arXiv:quant-ph/0502072 (https://arxiv.org/abs/quant-ph/0502072). Bibcode:2005quant.ph..2072A (https://ui.adsabs.harvard.edu/abs/2005quant.ph..2072A). See section 7 "Quantum Gravity": "[...] to anyone who wants a test or benchmark for a favorite quantum gravity theory,[author's footnote: That is, one without all the bother of making numerical predictions and comparing them to observation] let me humbly propose the following: *can you define Quantum Gravity Polynomial-Time?* [...] until we can say what it means for a 'user' to specify an 'input' and 'later' receive an 'output'—*there is no such thing as computation, not even theoretically.*" (emphasis in original)

15. "D-Wave Systems sells its first Quantum Computing System to Lockheed Martin Corporation" (https://web.archive.org/web/20201222041457/https://www.dwavesys.com/en/pressreleases.html#lm_2011). D-Wave. 25 May 2011. Archived from the original (http://www.dwavesys.com/en/pressreleases.html#lm_2011) on 22 December 2020. Retrieved 30 May 2011.

References

- Nielsen, Michael; Chuang, Isaac (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. ISBN 978-0-521-63503-5. OCLC 174527496 (https://search.worldcat.org/oclc/174527496).
- Arora, Sanjeev; Barak, Boaz (2016). *Computational Complexity: A Modern Approach* (https://archive.org/details/computationalcom00aror). Cambridge University Press. pp. 201 (https://archive.org/details/computationalcom00aror/page/n226)–236. ISBN 978-0-521-42426-4.
- Watrous, John (2008). "Quantum Computational Complexity". arXiv:0804.3401v1 (https://arxiv.org/abs/0804.3401v1) [quant-ph (https://arxiv.org/archive/quant-ph)].
- Watrous J. (2009) Quantum Computational Complexity (https://link.springer.com/referencework/10.1007/978-0-387-30440-3). In: Meyers R. (eds) Encyclopedia of Complexity and Systems Science. Springer, New York, NY

External links

- MIT lectures (https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-845-quantum-complexity-theory-fall-2010/) by Scott Aaronson

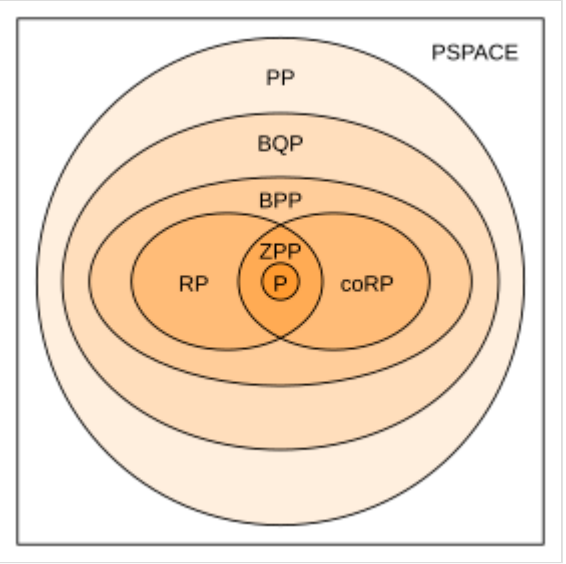
Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_complexity_theory&oldid=1181318945"

WIKIPEDIA
The Free Encyclopedia

BQP

In computational complexity theory, **bounded-error quantum polynomial time** (**BQP**) is the class of decision problems solvable by a quantum computer in polynomial time, with an error probability of at most 1/3 for all instances.[1] It is the quantum analogue to the complexity class **BPP**.

A decision problem is a member of **BQP** if there exists a quantum algorithm (an algorithm that runs on a quantum computer) that solves the decision problem with high probability and is guaranteed to run in polynomial time. A run of the algorithm will correctly solve the decision problem with a probability of at least 2/3.



BQP in relation to other probabilistic complexity classes (ZPP, RP, co-RP, BPP, PP), which generalise P within PSPACE. It is unknown if any of these containments are strict.

Definition

BQP can be viewed as the languages associated with certain bounded-error uniform families of quantum circuits.[1] A language L is in **BQP** if and only if there exists a polynomial-time uniform family of quantum circuits $\{Q_n : n \in \mathbb{N}\}$, such that

- For all $n \in \mathbb{N}$, Q_n takes n qubits as input and outputs 1 bit
- For all x in L, $\Pr(Q_{|x|}(x) = 1) \geq \frac{2}{3}$
- For all x not in L, $\Pr(Q_{|x|}(x) = 0) \geq \frac{2}{3}$

Alternatively, one can define **BQP** in terms of quantum Turing machines. A language L is in **BQP** if and only if there exists a polynomial quantum Turing machine that accepts L with an error probability of at most 1/3 for all instances.[2]

Similarly to other "bounded error" probabilistic classes, the choice of 1/3 in the definition is arbitrary. We can run the algorithm a constant number of times and take a

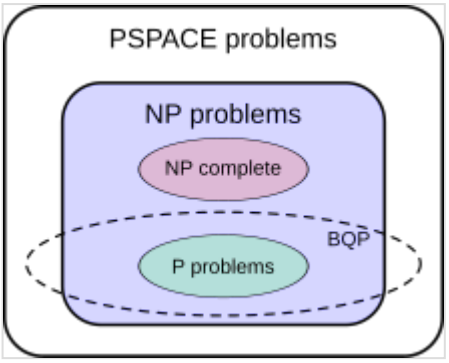
BQP algorithm (1 run)		
Correct answer \ **Answer produced**	**Yes**	**No**
Yes	≥ 2/3	≤ 1/3
No	≤ 1/3	≥ 2/3
BQP algorithm (*k* runs)		
Correct answer \ **Answer produced**	**Yes**	**No**
Yes	$> 1 - 2^{-ck}$	$< 2^{-ck}$
No	$< 2^{-ck}$	$> 1 - 2^{-ck}$
for some constant $c > 0$		

majority vote to achieve any desired probability of correctness less than 1, using the Chernoff bound. The complexity class is unchanged by allowing error as high as $1/2 - n^{-c}$ on the one hand, or requiring error as small as 2^{-n^c} on the other hand, where c is any positive constant, and n is the length of input.[3]

Relationship to other complexity classes

> **?** **Unsolved problem in computer science**:
> *What is the relationship between* **BQP** *and* **NP***?*
> (more unsolved problems in computer science)

BQP is defined for quantum computers; the corresponding complexity class for classical computers (or more formally for probabilistic Turing machines) is **BPP**. Just like **P** and **BPP**, **BQP** is low for itself, which means $\mathsf{BQP}^{\mathsf{BQP}} = \mathsf{BQP}$.[2] Informally, this is true because polynomial time algorithms are closed under composition. If a polynomial time algorithm calls polynomial time algorithms as subroutines, the resulting algorithm is still polynomial time.



The suspected relationship of **BQP** to other problem spaces[1]

BQP contains **P** and **BPP** and is contained in **AWPP**,[4] **PP**[5] and **PSPACE**.[2] In fact, **BQP** is low for **PP**, meaning that a **PP** machine achieves no benefit from being able to solve **BQP** problems instantly, an indication of the possible difference in power between these similar classes. The known relationships with classic complexity classes are:

$$\mathsf{P} \subseteq \mathsf{BPP} \subseteq \mathsf{BQP} \subseteq \mathsf{AWPP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP}$$

As the problem of $\mathsf{P} \stackrel{?}{=} \mathsf{PSPACE}$ has not yet been solved, the proof of inequality between **BQP** and classes mentioned above is supposed to be difficult.[2] The relation between **BQP** and **NP** is not known. In May 2018, computer scientists Ran Raz of Princeton University and Avishay Tal of Stanford University published a paper[6] which showed that, relative to an oracle, BQP was not contained in PH. It can be proven that there exists an oracle A such that $\mathsf{BQP}^{\mathbf{A}} \not\subseteq \mathsf{PH}^{\mathbf{A}}$.[7] In an extremely informal sense, this can be thought of as giving PH and BQP an identical, but additional, capability and verifying that BQP with the oracle ($\mathrm{BQP}^{\mathrm{A}}$) can do things PH^{A} cannot. While an oracle separation has been proven, the fact that BQP is not contained in PH has not been proven. An oracle separation does not prove whether or not complexity classes are the same. The oracle separation gives intuition that BQP may not be contained in PH.

It has been suspected for many years that Fourier Sampling is a problem that exists within BQP, but not within the polynomial hierarchy. Recent conjectures have provided evidence that a similar problem, Fourier Checking, also exists in the class BQP without being contained in the polynomial hierarchy. This conjecture is especially notable because it suggests that problems existing in BQP could be classified as harder than NP-Complete problems. Paired with the fact that many practical BQP problems are suspected to exist outside of P (it is suspected and not verified because there is no proof that P ≠ NP), this illustrates the potential power of quantum computing in relation to classical computing.[7]

Adding postselection to **BQP** results in the complexity class **PostBQP** which is equal to **PP**.[8][9]

A complete problem for Promise-BQP

Promise-BQP is the class of promise problems that can be solved by a uniform family of quantum circuits (i.e., within BQP).[10] Completeness proofs focus on this version of BQP. Similar to the notion of NP-completeness and other complete problems, we can define a complete problem as a problem that is in Promise-BQP and that every other problem in Promise-BQP reduces to it in polynomial time.

APPROX-QCIRCUIT-PROB

The APPROX-QCIRCUIT-PROB problem is complete for efficient quantum computation, and the version presented below is complete for the Promise-BQP complexity class (and not for the total BQP complexity class, for which no complete problems are known). APPROX-QCIRCUIT-PROB's completeness makes it useful for proofs showing the relationships between other complexity classes and BQP.

Given a description of a quantum circuit C acting on n qubits with m gates, where m is a polynomial in n and each gate acts on one or two qubits, and two numbers $\alpha, \beta \in [0,1], \alpha > \beta$, distinguish between the following two cases:

- measuring the first qubit of the state $C|0\rangle^{\otimes n}$ yields $|1\rangle$ with probability $\geq \alpha$
- measuring the first qubit of the state $C|0\rangle^{\otimes n}$ yields $|1\rangle$ with probability $\leq \beta$

Here, there is a promise on the inputs as the problem does not specify the behavior if an instance is not covered by these two cases.

Claim. Any BQP problem reduces to APPROX-QCIRCUIT-PROB.

Proof. Suppose we have an algorithm A that solves APPROX-QCIRCUIT-PROB, i.e., given a quantum circuit C acting on n qubits, and two numbers $\alpha, \beta \in [0,1], \alpha > \beta$, A distinguishes between the above two cases. We can solve any problem in BQP with this oracle, by setting $\alpha = 2/3, \beta = 1/3$.

For any $L \in \mathsf{BQP}$, there exists family of quantum circuits $\{Q_n : n \in \mathbb{N}\}$ such that for all $n \in \mathbb{N}$, a state $|x\rangle$ of n qubits, if $x \in L, Pr(Q_n(|x\rangle) = 1) \geq 2/3$; else if $x \notin L, Pr(Q_n(|x\rangle) = 0) \geq 2/3$. Fix an input $|x\rangle$ of n qubits, and the corresponding quantum circuit Q_n. We can first construct a circuit C_x such that $C_x|0\rangle^{\otimes n} = |x\rangle$. This can be done easily by hardwiring $|x\rangle$ and apply a sequence of CNOT gates to flip the qubits. Then we can combine two circuits to get $C' = Q_n C_x$, and now $C'|0\rangle^{\otimes n} = Q_n|x\rangle$. And finally, necessarily the results of Q_n is obtained by measuring several qubits and apply some (classical) logic gates to them. We can always defer the measurement[11][12] and reroute the circuits so that by measuring the first qubit of $C'|0\rangle^{\otimes n} = Q_n|x\rangle$, we get the output. This will be our circuit C, and we decide the membership of $x \in L$ by running $A(C)$ with $\alpha = 2/3, \beta = 1/3$. By definition of BQP, we will either fall into the first case (acceptance), or the second case (rejection), so $L \in \mathsf{BQP}$ reduces to APPROX-QCIRCUIT-PROB.

BQP and EXP

We begin with an easier containment. To show that $\mathsf{BQP} \subseteq \mathsf{EXP}$, it suffices to show that APPROX-QCIRCUIT-PROB is in EXP since APPROX-QCIRCUIT-PROB is BQP-complete.

Claim — $\text{APPROX-QCIRCUIT-PROB} \in \mathsf{EXP}$

Proof

The idea is simple. Since we have exponential power, given a quantum circuit C, we can use classical computer to stimulate each gate in C to get the final state.

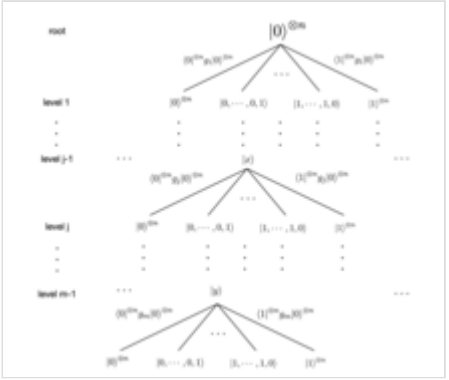
More formally, let C be a polynomial sized quantum circuit on n qubits and m gates, where m is polynomial in n. Let $|\psi_0\rangle = |0\rangle^{\otimes n}$ and $|\psi_i\rangle$ be the state after the i-th gate in the circuit is applied to $|\psi_{i-1}\rangle$. Each state $|\psi_i\rangle$ can be represented in a classical computer as a unit vector in $\mathbb{C}^{2^n}$. Furthermore, each gate can be represented by a matrix in $\mathbb{C}^{2^n \times 2^n}$. Hence, the final state $|\psi_m\rangle$ can be computed in $O(m \cdot 2^{2n})$ time, and therefore all together, we have an $2^{O(n)}$ time algorithm for calculating the final state, and thus the probability that the first qubit is measured to be one. This implies that $\text{APPROX-QCIRCUIT-PROB} \in \mathsf{EXP}$.

Note that this algorithm also requires $2^{O(n)}$ space to store the vectors and the matrices. We will show in the following section that we can improve upon the space complexity.

BQP and PSPACE

Sum of histories is a technique introduced by physicist Richard Feynman for path integral formulation. APPROX-QCIRCUIT-PROB can be formulated in the sum of histories technique to show that $\mathsf{BQP} \subseteq \mathsf{PSPACE}$.[13]

Consider a quantum circuit C, which consists of t gates, $g_1, g_2, \cdots, g_m$, where each g_j comes from a universal gate set and acts on at most two qubits. To understand what the sum of histories is, we visualize the evolution of a quantum state given a quantum circuit as a tree. The root is the input $|0\rangle^{\otimes n}$, and each node in the tree has 2^n children, each representing a state in $\mathbb{C}^n$. The weight on a tree edge from a node in j-th level representing a state $|x\rangle$ to a node in $j+1$-th level representing a state $|y\rangle$ is $\langle y|g_{j+1}|x\rangle$, the amplitude of $|y\rangle$ after applying g_{j+1} on $|x\rangle$. The transition amplitude of a root-to-leaf path is the product of all the weights on the edges along the path. To get the probability of the final state being $|\psi\rangle$, we sum up the amplitudes of all root-to-leave paths that ends at a node representing $|\psi\rangle$.



Sum of Histories Tree

More formally, for the quantum circuit C, its sum over histories tree is a tree of depth m, with one level for each gate g_i in addition to the root, and with branching factor 2^n.

Define — A history is a path in the sum of histories tree. We will denote a history by a sequence $(u_0 = |0\rangle^{\otimes n} \to u_1 \to \cdots \to u_{m-1} \to u_m = x)$ for some final state x.

Define — Let $u, v \in \{0,1\}^n$. Let amplitude of the edge $(|u\rangle, |v\rangle)$ in the j-th level of the sum over histories tree be $\alpha_j(u \to v) = \langle v|g_j|u\rangle$. For any history $h = (u_0 \to u_1 \to \cdots \to u_{m-1} \to u_m)$, the transition amplitude of the history is the product $\alpha_h = \alpha_1(|0\rangle^{\otimes n} \to u_1)\alpha_2(u_1 \to u_2)\cdots\alpha_m(u_{m-1} \to x)$.

Claim — For a history $(u_0 \to \cdots \to u_m)$. The transition amplitude of the history is computable in polynomial time.

Proof

Each gate g_j can be decomposed into $g_j = I \otimes \tilde{g}_j$ for some unitary operator $\tilde{g}_j$ acting on two qubits, which without loss of generality can be taken to be the first two. Hence, $\langle v|g_j|u\rangle = \langle v_1, v_2|\tilde{g}_j|u_1, u_2\rangle\langle v_3, \cdots, v_n|u_3, \cdots, u_n\rangle$ which can be computed in polynomial time in n. Since m is polynomial in n, the transition amplitude of the history can be computed in polynomial time.

Claim — Let $C|0\rangle^{\otimes n} = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ be the final state of the quantum circuit. For some $x \in \{0,1\}^n$, the amplitude α_x can be computed by $\alpha_x = \sum_{h=(|0\rangle^{\otimes n}\to u_1\to\cdots\to u_{t-1}\to|x\rangle)} \alpha_h$.

Proof

We have $\alpha_x = \langle x|C|0\rangle^{\otimes n} = \langle x|g_t g_{t-1}\cdots g_1|C|0\rangle^{\otimes n}$. The result comes directly by inserting $I = \sum_{x\in\{0,1\}^n} |x\rangle\langle x|$ between g_1, g_2, and g_2, g_3, and so on, and then expand out the equation. Then each term corresponds to a α_h, where $h = (|0\rangle^{\otimes n} \to u_1 \to \cdots \to u_{t-1} \to |x\rangle)$

Claim — APPROX-QCIRCUIT-PROB $\in$ PSPACE

Notice in the sum over histories algorithm to compute some amplitude α_x, only one history is stored at any point in the computation. Hence, the sum over histories algorithm uses $O(nm)$ space to compute α_x for any x since $O(nm)$ bits are needed to store the histories in addition to some workspace variables.

Therefore, in polynomial space, we may compute $\sum_x |\alpha_x|^2$ over all x with the first qubit being 1, which is the probability that the first qubit is measured to be 1 by the end of the circuit.

Notice that compared with the simulation given for the proof that $\mathsf{BQP} \subseteq \mathsf{EXP}$, our algorithm here takes far less space but far more time instead. In fact it takes $O(m \cdot 2^{mn})$ time to calculate a single amplitude!

BQP and PP

A similar sum-over-histories argument can be used to show that $\mathsf{BQP} \subseteq \mathsf{PP}$. [14]

P and BQP

We know $\mathsf{P} \subseteq \mathsf{BQP}$, since every classical circuit can be simulated by a quantum circuit. [15]

It is conjectured that BQP solves hard problems outside of P, specifically, problems in NP. The claim is indefinite because we don't know if P=NP, so we don't know if those problems are actually in P. Below are some evidence of the conjecture:

- Integer factorization (see Shor's algorithm)[16]
- Discrete logarithm[16]
- Simulation of quantum systems (see universal quantum simulator)
- Approximating the Jones polynomial at certain roots of unity
- Harrow-Hassidim-Lloyd (HHL) algorithm

See also

- Hidden subgroup problem
- Polynomial hierarchy (PH)
- Quantum complexity theory
- **QMA**, the quantum equivalent to **NP**.
- QIP, the quantum equivalent to IP.

References

1. Michael Nielsen and Isaac Chuang (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. ISBN 0-521-63503-9.
2. Bernstein, Ethan; Vazirani, Umesh (October 1997). "Quantum Complexity Theory". *SIAM Journal on Computing*. **26** (5): 1411–1473. CiteSeerX 10.1.1.655.1186 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.655.1186). doi:10.1137/S0097539796300921 (https://doi.org/10.1137%2FS0097539796300921).
3. Barak, Sanjeev Arora, Boaz (2009). *Computational Complexity: A Modern Approach / Sanjeev Arora and Boaz Barak* (https://www.cs.princeton.edu/theory/complexity/). Cambridge. p. 122. Retrieved 24 July 2018.

4. Fortnow, Lance; Rogers, John (1999). "Complexity limitations on Quantum computation" (http://people.cs.uchicago.edu/~fortnow/papers/quantum.pdf) (PDF). *J. Comput. Syst. Sci*. **59** (2): 240–252. arXiv:cs/9811023 (https://arxiv.org/abs/cs/9811023). doi:10.1006/jcss.1999.1651 (https://doi.org/10.1006%2Fjcss.1999.1651). ISSN 0022-0000 (https://search.worldcat.org/issn/0022-0000). S2CID 42516312 (https://api.semanticscholar.org/CorpusID:42516312). Archived (https://ghostarchive.org/archive/20221009/http://people.cs.uchicago.edu/~fortnow/papers/quantum.pdf) (PDF) from the original on 2022-10-09.
5. L. Adleman, J. DeMarrais, and M.-D. Huang. Quantum computability. SIAM J. Comput., 26(5):1524–1540, 1997.
6. George, Michael Goderbauer, Stefan. "ECCC - TR18-107" (https://eccc.weizmann.ac.il/report/2018/107/). *eccc.weizmann.ac.il*. Retrieved 2018-08-03.
7. Aaronson, Scott (2010). "BQP and the Polynomial Hierarchy" (https://www.scottaaronson.com/papers/bqpph.pdf) (PDF). *Proceedings of ACM STOC 2010*. Archived (https://ghostarchive.org/archive/20221009/https://www.scottaaronson.com/papers/bqpph.pdf) (PDF) from the original on 2022-10-09.
8. Aaronson, Scott (2005). "Quantum computing, postselection, and probabilistic polynomial-time". *Proceedings of the Royal Society A*. **461** (2063): 3473–3482. arXiv:quant-ph/0412187 (https://arxiv.org/abs/quant-ph/0412187). Bibcode:2005RSPSA.461.3473A (https://ui.adsabs.harvard.edu/abs/2005RSPSA.461.3473A). doi:10.1098/rspa.2005.1546 (https://doi.org/10.1098%2Frspa.2005.1546). S2CID 1770389 (https://api.semanticscholar.org/CorpusID:1770389).. Preprint available at [1] (https://arxiv.org/abs/quant-ph/0412187)
9. Aaronson, Scott (2004-01-11). "Complexity Class of the Week: PP" (http://weblog.fortnow.com/2004/01/complexity-class-of-week-pp-by-guest.html). *Computational Complexity Weblog*. Retrieved 2008-05-02.
10. Janzing, Dominik; Wocjan, Pawel (2007-03-30). "A Simple PromiseBQP-complete Matrix Problem" (https://theoryofcomputing.org/articles/v003a004/v003a004.pdf) (PDF). *Theory of Computing*. **3** (4): 61–79. doi:10.4086/toc.2007.v003a004 (https://doi.org/10.4086%2Ftoc.2007.v003a004). Retrieved 2024-04-18.
11. Michael A. Nielsen; Isaac L. Chuang (9 December 2010). "4.4 Measurement". *Quantum Computation and Quantum Information: 10th Anniversary Edition* (https://books.google.com/books?id=-s4DEy7o-a0C). Cambridge University Press. p. 186. ISBN 978-1-139-49548-6.
12. Odel A. Cross (5 November 2012). "5.2.2 Deferred Measurement". *Topics in Quantum Computing* (https://books.google.com/books?id=b_D9flK2h8QC&pg=PA348). O. A. Cross. p. 348. ISBN 978-1-4800-2749-7.
13. E. Bernstein and U. Vazirani. Quantum complexity theory, SIAM Journal on Computing, 26(5):1411-1473, 1997.
14. L. Adleman, J. DeMarrais, and M. Huang. Quantum computability, SIAM Journal on Computing 26:1524-1540, 1997.
15. Nielsen, Michael A.; Chuang, Isaac L. (2000), Quantum Computation and Quantum Information, Cambridge: Cambridge University Press, ISBN 0-521-63235-8, MR 1796805.
16. arXiv:quant-ph/9508027v2 *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, Peter W. Shor (http://www.arxiv.org/abs/quant-ph/9508027)

External links

- Complexity Zoo link to BQP (https://complexityzoo.uwaterloo.ca/Complexity_Zoo:B#bqp) Archived (https://web.archive.org/web/20130603134129/https://complexityzoo.uwaterloo.ca/Complexity_Zoo:B#bqp) 2013-06-03 at the Wayback Machine

Retrieved from "https://en.wikipedia.org/w/index.php?title=BQP&oldid=1230041542"

WIKIPEDIA
The Free Encyclopedia

Exact quantum polynomial time

In computational complexity theory, **exact quantum polynomial time** (**EQP** or sometimes **QP**) is the class of decision problems that can be solved by a quantum computer with zero error probability and in guaranteed worst-case polynomial time. It is the quantum analogue of the complexity class P. This is in contrast to bounded-error quantum computing, where quantum algorithms are expected to run in polynomial time, but may not always do so.

In the original definition of EQP, each language was computed by a single quantum Turing machine (QTM), using a finite gate set whose amplitudes could be computed in polynomial time. However, some results have required the use of an infinite gate set. The amplitudes in the gate set are typically algebraic numbers.

References

- *Complexity Zoo*: EQP (https://complexityzoo.net/Complexity_Zoo:E#eqp)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Exact_quantum_polynomial_time&oldid=1141428076"

WIKIPEDIA
The Free Encyclopedia

QIP (complexity)

In computational complexity theory, the class **QIP** (which stands for **Quantum Interactive Polynomial time**) is the quantum computing analogue of the classical complexity class IP, which is the set of problems solvable by an interactive proof system with a polynomial-time verifier and one computationally unbounded prover. Informally, IP is the set of languages for which a computationally unbounded prover can convince a polynomial-time verifier to accept when the input is in the language (with high probability) and cannot convince the verifier to accept when the input is not in the language (again, with high probability). In other words, the prover and verifier may interact for polynomially many rounds, and if the input is in the language the verifier should accept with probability greater than 2/3, and if the input is not in the language, the verifier should be reject with probability greater than 2/3. In IP, the verifier is like a BPP machine. In QIP, the communication between the prover and verifier is quantum, and the verifier can perform quantum computation. In this case the verifier is like a BQP machine.

By restricting the number of messages used in the protocol to at most *k*, we get the complexity class QIP(k). QIP and QIP(k) were introduced by John Watrous,[1] who along with Kitaev proved in a later paper[2] that QIP = QIP(3), which shows that 3 messages are sufficient to simulate a polynomial-round quantum interactive protocol. Since QIP(3) is already QIP, this leaves 4 possibly different classes: QIP(0), which is BQP, QIP(1), which is QMA, QIP(2) and QIP.

Kitaev and Watrous also showed that QIP is contained in EXP, the class of problems solvable by a deterministic Turing machine in exponential time.[2] QIP(2) was then shown to be contained in PSPACE, the set of problems solvable by a deterministic Turing machine in polynomial space.[3] Both results were subsumed by the 2009 result that QIP is contained in PSPACE,[4] which also proves that QIP = IP = PSPACE, since PSPACE is easily shown to be in QIP using the result IP = PSPACE.

References

1. Watrous, John (2003), "PSPACE has constant-round quantum interactive proof systems", *Theor. Comput. Sci.*, **292** (3), Essex, UK: Elsevier Science Publishers Ltd.: 575–588, doi:10.1016/S0304-3975(01)00375-9 (https://doi.org/10.1016%2FS0304-3975%2801%2900375-9), ISSN 0304-3975 (https://search.worldcat.org/issn/0304-3975)
2. Kitaev, Alexei; Watrous, John (2000), "Parallelization, amplification, and exponential time simulation of quantum interactive proof systems", *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, ACM, pp. 608–617, ISBN 978-1-58113-184-0
3. Jain, Rahul; Upadhyay, Sarvagya; Watrous, John (2009), "Two-Message Quantum Interactive Proofs Are in PSPACE", *FOCS '09: Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, IEEE Computer Society, pp. 534–543, ISBN 978-0-7695-3850-1

4. Jain, Rahul; Ji, Zhengfeng; Upadhyay, Sarvagya; Watrous, John (2010), "QIP = PSPACE", *STOC '10: Proceedings of the 42nd ACM symposium on Theory of computing*, ACM, pp. 573–582, ISBN 978-1-4503-0050-6

External links

- *Complexity Zoo*: QIP (https://complexityzoo.net/Complexity_Zoo:Q#qip)

Retrieved from "https://en.wikipedia.org/w/index.php?title=QIP_(complexity)&oldid=1221466312"

WIKIPEDIA
The Free Encyclopedia

QMA

In computational complexity theory, **QMA**, which stands for **Quantum Merlin Arthur**, is the set of languages for which, when a string is in the language, there is a polynomial-size quantum proof (a quantum state) that convinces a polynomial time quantum verifier (running on a quantum computer) of this fact with high probability. Moreover, when the string is not in the language, every polynomial-size quantum state is rejected by the verifier with high probability.

The relationship between QMA and BQP is analogous to the relationship between complexity classes NP and P. It is also analogous to the relationship between the probabilistic complexity class MA and BPP.

QAM is a related complexity class, in which fictional agents Arthur and Merlin carry out the sequence: Arthur generates a random string, Merlin answers with a quantum certificate and Arthur verifies it as a BQP machine.

Definition

A language L is in $\mathsf{QMA}(c, s)$ if there exists a polynomial time quantum verifier V and a polynomial $p(x)$ such that:[1][2][3]

- $\forall x \in L$, there exists a quantum state $|\psi\rangle$ such that the probability that V accepts the input $(|x\rangle, |\psi\rangle)$ is greater than c.
- $\forall x \notin L$, for all quantum states $|\psi\rangle$, the probability that V accepts the input $(|x\rangle, |\psi\rangle)$ is less than s.

where $|\psi\rangle$ ranges over all quantum states with at most $p(|x|)$ qubits.

The complexity class QMA is defined to be equal to $\mathsf{QMA}(2/3, 1/3)$. However, the constants are not too important since the class remains unchanged if c and s are set to any constants such that c is greater than s. Moreover, for any polynomials $q(n)$ and $r(n)$, we have

$$\mathsf{QMA}\left(\frac{2}{3}, \frac{1}{3}\right) = \mathsf{QMA}\left(\frac{1}{2} + \frac{1}{q(n)}, \frac{1}{2} - \frac{1}{q(n)}\right) = \mathsf{QMA}(1 - 2^{-r(n)}, 2^{-r(n)}).$$

Problems in QMA

Since many interesting classes are contained in QMA, such as P, BQP and NP, all problems in those classes are also in QMA. However, there are problems that are in QMA but not known to be in NP or BQP. Some such well known problems are discussed below.

A problem is said to be QMA-hard, analogous to NP-hard, if every problem in QMA can be reduced to it. A problem is said to be QMA-complete if it is QMA-hard and in QMA.

The local Hamiltonian problem

A k-local Hamiltonian (quantum mechanics) H is a Hermitian matrix acting on n qubits which can be represented as the sum of m Hamiltonian Terms acting upon at most k qubits each.

$$H = \sum_{i=1}^{m} H_i$$

The general k-local Hamiltonian problem is, given a k-local Hamiltonian H, to find the smallest eigenvalue λ of H.[4] λ is also called the ground state energy of the Hamiltonian.

The decision version of the k-local Hamiltonian problem is a type of promise problem and is defined as, given a k-local Hamiltonian and α, β where $\alpha > \beta$, to decide if there exists a quantum eigenstate $|\psi\rangle$ of H with associated eigenvalue λ, such that $\lambda \leq \beta$ or if $\lambda \geq \alpha$.

The local Hamiltonian problem is the quantum analogue of MAX-SAT. The k-local Hamiltonian problem is QMA-complete for k ≥ 2.[5]

The 2-local Hamiltonian problem restricted to act on a two dimensional grid of qubits, is also QMA-complete.[6] It has been shown that the k-local Hamiltonian problem is still QMA-hard even for Hamiltonians representing a 1-dimensional line of particles with nearest-neighbor interactions with 12 states per particle.[7] If the system is translationally-invariant, its local Hamiltonian problem becomes $\mathrm{QMA_{EXP}}$-complete (as the problem input is encoded in the system size, the verifier now has exponential runtime while maintaining the same promise gap).[8][9]

QMA-hardness results are known for simple lattice models of qubits such as the ZX Hamiltonian [10] $H_{ZX} = \sum_i h_i Z_i + \sum_i \Delta_i X_i + \sum_{i<j} J^{ij} Z_i Z_j + \sum_{i<j} K^{ij} X_i X_j$ where Z, X represent the Pauli matrices σ_z, σ_x. Such models are applicable to universal adiabatic quantum computation.

k-local Hamiltonians problems are analogous to classical Constraint Satisfaction Problems.[11] The following table illustrates the analogous gadgets between classical CSPs and Hamiltonians.

Classical	Quantum	Notes
Constraint Satisfaction Problem	Hamiltonian	
Variable	Qubit	
Constraint	Hamiltonian Term	
Variable Assignment	Quantum state	
Number of constraints satisfied	Hamiltonian's energy term	
Optimal Solution	Hamiltonian's ground state	The most possible constraints satisfied

Other QMA-complete problems

A list of known QMA-complete problems can be found at https://arxiv.org/abs/1212.6312.

Related classes

QCMA (or **MQA**[2]), which stands for Quantum Classical Merlin Arthur (or Merlin Quantum Arthur), is similar to QMA, but the proof has to be a classical string. It is not known whether QMA equals QCMA, although QCMA is clearly contained in QMA.

QIP(k), which stands for Quantum Interactive Polynomial time (k messages), is a generalization of QMA where Merlin and Arthur can interact for k rounds. QMA is QIP(1). QIP(2) is known to be in PSPACE.[12]

QIP is QIP(k) where k is allowed to be polynomial in the number of qubits. It is known that QIP(3) = QIP.[13] It is also known that QIP = IP = PSPACE.[14]

Relationship to other classes

QMA is related to other known complexity classes by the following relations:

$$\mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{QCMA} \subseteq \mathsf{QMA} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE}$$

The first inclusion follows from the definition of NP. The next two inclusions follow from the fact that the verifier is being made more powerful in each case. QCMA is contained in QMA since the verifier can force the prover to send a classical proof by measuring proofs as soon as they are received. The fact that QMA is contained in PP was shown by Alexei Kitaev and John Watrous. PP is also easily shown to be in PSPACE.

It is unknown if any of these inclusions is unconditionally strict, as it is not even known whether P is strictly contained in PSPACE or P = PSPACE. However, the currently best known upper bounds on QMA are [15] [16]

$$\mathsf{QMA} \subseteq \mathsf{A_0PP} \text{ and } \mathsf{QMA} \subseteq \mathsf{P}^{\mathsf{QMA[log]}},$$

where both $\mathsf{A_0PP}$ and $\mathsf{P}^{\mathsf{QMA[log]}}$ are contained in PP. It is unlikely that QMA equals $\mathsf{P}^{\mathsf{QMA[log]}}$, as this would imply $\mathsf{QMA} = \mathsf{co\text{-}QMA}$. It is unknown whether $\mathsf{P}^{\mathsf{QMA[log]}} \subseteq \mathsf{A_0PP}$ or vice versa.

References

1. Aharonov, Dorit; Naveh, Tomer (2002). "Quantum NP – A Survey". arXiv:quant-ph/0210077v1 (https://arxiv.org/abs/quant-ph/0210077v1).
2. Watrous, John (2009). "Quantum Computational Complexity". In Meyers, Robert A. (ed.). *Encyclopedia of Complexity and Systems Science*. pp. 7174–7201. arXiv:0804.3401 (https://arxiv.org/abs/0804.3401). doi:10.1007/978-0-387-30440-3_428 (https://doi.org/10.1007%2F978-0-387-30440-3_428). ISBN 978-0-387-75888-6. S2CID 1380135 (https://api.semanticscholar.org/CorpusID:1380135).

3. Gharibian, Sevag; Huang, Yichen; Landau, Zeph; Shin, Seung Woo (2015). "Quantum Hamiltonian Complexity". *Foundations and Trends in Theoretical Computer Science*. **10** (3): 159–282. arXiv:1401.3916 (https://arxiv.org/abs/1401.3916). doi:10.1561/0400000066 (https://doi.org/10.1561%2F0400000066). S2CID 47494978 (https://api.semanticscholar.org/CorpusID:47494978).
4. O'Donnel, Ryan. "Lecture 24: QMA: Quantum Merlin Arthur" (https://www.cs.cmu.edu/~odonnell/quantum15/lecture24.pdf) (PDF). Retrieved 18 April 2021.
5. Kempe, Julia; Kitaev, Alexei; Regev, Oded (2006). "The complexity of the local Hamiltonian problem". *SIAM Journal on Computing*. **35** (5): 1070–1097. arXiv:quant-ph/0406180v2 (https://arxiv.org/abs/quant-ph/0406180v2). doi:10.1137/S0097539704445226 (https://doi.org/10.1137%2FS0097539704445226)..
6. Oliveira, Roberto; Terhal, Barbara M. (2008). "The complexity of quantum spin systems on a two-dimensional square lattice". *Quantum Information and Computation*. **8** (10): 900–924. arXiv:quant-ph/0504050 (https://arxiv.org/abs/quant-ph/0504050). Bibcode:2005quant.ph..4050O (https://ui.adsabs.harvard.edu/abs/2005quant.ph..4050O). doi:10.26421/QIC8.10-2 (https://doi.org/10.26421%2FQIC8.10-2). S2CID 3262293 (https://api.semanticscholar.org/CorpusID:3262293).
7. Aharonov, Dorit; Gottesman, Daniel; Irani, Sandy; Kempe, Julia (2009). "The power of quantum systems on a line". *Communications in Mathematical Physics*. **287** (1): 41–65. arXiv:0705.4077 (https://arxiv.org/abs/0705.4077). Bibcode:2009CMaPh.287...41A (https://ui.adsabs.harvard.edu/abs/2009CMaPh.287...41A). doi:10.1007/s00220-008-0710-3 (https://doi.org/10.1007%2Fs00220-008-0710-3). S2CID 1916001 (https://api.semanticscholar.org/CorpusID:1916001).
8. Aharonov, Dorit; Gottesman, Daniel; Irani, Sandy; Kempe, Julia (1 April 2009). "The Power of Quantum Systems on a Line". *Communications in Mathematical Physics*. **287** (1): 41–65. CiteSeerX 10.1.1.320.7377 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.320.7377). doi:10.1007/s00220-008-0710-3 (https://doi.org/10.1007%2Fs00220-008-0710-3). S2CID 1916001 (https://api.semanticscholar.org/CorpusID:1916001).
9. Bausch, Johannes; Cubitt, Toby; Ozols, Maris (November 2017). "The Complexity of Translationally Invariant Spin Chains with Low Local Dimension" (https://doi.org/10.1007%2Fs00023-017-0609-7). *Annales Henri Poincaré*. **18** (11): 3449–3513. arXiv:1605.01718 (https://arxiv.org/abs/1605.01718). doi:10.1007/s00023-017-0609-7 (https://doi.org/10.1007%2Fs00023-017-0609-7).
10. Biamonte, Jacob; Love, Peter (2008). "Realizable Hamiltonians for universal adiabatic quantum computers". *Physical Review A*. **78** (1): 012352. arXiv:0704.1287 (https://arxiv.org/abs/0704.1287). Bibcode:2008PhRvA..78a2352B (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78a2352B). doi:10.1103/PhysRevA.78.012352 (https://doi.org/10.1103%2FPhysRevA.78.012352). S2CID 9859204 (https://api.semanticscholar.org/CorpusID:9859204)..
11. Yuen, Henry. "The Complexity of Entanglement" (http://henryyuen.net/fall2020/complexity_of_entanglement_notes.pdf) (PDF). *henryyuen.net*. Retrieved 20 April 2021.
12. Jain, Rahul; Upadhyay, Sarvagya; Watrous, John (2009). "Two-message quantum interactive proofs are in PSPACE". *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS '09)*. IEEE Computer Society. pp. 534–543. arXiv:0905.1300 (https://arxiv.org/abs/0905.1300). doi:10.1109/FOCS.2009.30 (https://doi.org/10.1109%2FFOCS.2009.30). ISBN 978-0-7695-3850-1. S2CID 6869749 (https://api.semanticscholar.org/CorpusID:6869749).
13. Watrous, John (2003). "PSPACE has constant-round quantum interactive proof systems" (https://doi.org/10.1016%2FS0304-3975%2801%2900375-9). *Theoretical Computer Science*. **292** (3): 575–588. doi:10.1016/S0304-3975(01)00375-9 (https://doi.org/10.1016%2FS0304-3975%2801%2900375-9).

14. Jain, Rahul; Ji, Zhengfeng; Upadhyay, Sarvagya; Watrous, John (2011). "QIP = PSPACE". *Journal of the ACM*. **58** (6): A30. doi:10.1145/2049697.2049704 (https://doi.org/10.1145%2F2049697.2049704). S2CID 265099379 (https://api.semanticscholar.org/CorpusID:265099379).
15. Vyalyi, Mikhail N. (2003). "QMA = PP implies that PP contains PH" (https://eccc.weizmann.ac.il/eccc-reports/2003/TR03-021/index.html). *Electronic Colloquium on Computational Complexity*.
16. Gharibian, Sevag; Yirka, Justin (2019). "The complexity of simulating local measurements on quantum systems" (https://doi.org/10.22331%2Fq-2019-09-30-189). *Quantum*. **3**: 189. arXiv:1606.05626 (https://arxiv.org/abs/1606.05626). doi:10.22331/q-2019-09-30-189 (https://doi.org/10.22331%2Fq-2019-09-30-189).

External links

- Aaronson, Scott. "PHYS771 Lecture 13: How Big are Quantum States?" (http://www.scottaaronson.com/democritus/lec13.html).
- Gharibian, Sevag. "Lecture 5: Quantum Merlin Arthur (QMA) and strong error reduction" (http://groups.uni-paderborn.de/fg-qi/courses/UPB_QCOMPLEXITY/2019/notes/Lecture%205%20-%20Quantum%20Merlin%20Arthur%20(QMA)%20and%20strong%20error%20reduction.pdf) (PDF).
- *Complexity Zoo*: QMA (https://complexityzoo.net/Complexity_Zoo:Q#qma)

Retrieved from "https://en.wikipedia.org/w/index.php?title=QMA&oldid=1193722468"

WIKIPEDIA
The Free Encyclopedia

PostBQP

In computational complexity theory, **PostBQP** is a complexity class consisting of all of the computational problems solvable in polynomial time on a quantum Turing machine with postselection and bounded error (in the sense that the algorithm is correct at least 2/3 of the time on all inputs).

Postselection is not considered to be a feature that a realistic computer (even a quantum one) would possess, but nevertheless postselecting machines are interesting from a theoretical perspective.

Removing either one of the two main features (quantumness, postselection) from **PostBQP** gives the following two complexity classes, both of which are subsets of **PostBQP**:

- **BQP** is the same as **PostBQP** except without postselection
- $\mathbf{BPP_{path}}$ is the same as **PostBQP** except that instead of quantum, the algorithm is a classical randomized algorithm (with postselection)[1]

The addition of postselection seems to make quantum Turing machines much more powerful: Scott Aaronson proved[2][3] **PostBQP** is equal to **PP**, a class which is believed to be relatively powerful, whereas **BQP** is not known even to contain the seemingly smaller class **NP**. Using similar techniques, Aaronson also proved that small changes to the laws of quantum computing would have significant effects. As specific examples, under either of the two following changes, the "new" version of **BQP** would equal **PP**:

- if we broadened the definition of 'quantum gate' to include not just unitary operations but linear operations, or
- if the probability of measuring a basis state $|x\rangle$ was proportional to $|\alpha_x|^p$ instead of $|\alpha_x|^2$ for any even integer $p > 2$.

Basic properties

In order to describe some of the properties of **PostBQP** we fix a formal way of describing quantum postselection. Define a quantum algorithm to be a family of quantum circuits (specifically, a uniform circuit family). We designate one qubit as the *postselection qubit P* and another as the *output qubit Q*. Then **PostBQP** is defined by postselecting upon the event that the postselection qubit is $|1\rangle$. Explicitly, a language L is in PostBQP if there is a quantum algorithm A so that after running A on input x and measuring the two qubits P and Q,

- $P = 1$ with nonzero probability
- if the input x is in L then $\Pr[Q = 1|P = 1] \geq 2/3$
- if the input x is not in L then $\Pr[Q = 0|P = 1] \geq 2/3$.

One can show that allowing a single postselection step at the end of the algorithm (as described above) or allowing intermediate postselection steps during the algorithm are equivalent.[2][4]

Here are three basic properties of **PostBQP** (which also hold for **BQP** via similar proofs):

1. **PostBQP** is *closed under complement*. Given a language *L* in **PostBQP** and a corresponding deciding circuit family, create a new circuit family by flipping the output qubit after measurement, then the new circuit family proves the complement of *L* is in **PostBQP**.
2. You can do *probability amplification* in **PostBQP**. The definition of **PostBQP** is not changed if we replace the 2/3 value in its definition by any other constant strictly between 1/2 and 1. As an example, given a **PostBQP** algorithm *A* with success probability 2/3, we can construct another algorithm which runs three independent copies of *A*, outputs a postselection bit equal to the conjunction of the three "inner" ones, and outputs an output bit equal to the majority of the three "inner" ones; the new algorithm will be correct with conditional probability $(2/3)^3 + 3(1/3)(2/3)^2 = 20/27$, greater than the original 2/3.
3. **PostBQP** is *closed under intersection*. Suppose we have **PostBQP** circuit families for two languages L_1 and L_2, with respective postselection qubits and output qubits P_1, P_2, Q_1, Q_2. We may assume by probability amplification that both circuit families have success probability at least 5/6. Then we create a composite algorithm where the circuits for L_1 and L_2 are run independently, and we set *P* to the conjunction of P_1 and P_2, and *Q* to the conjunction of Q_1 and Q_2. It is not hard to see by a union bound that this composite algorithm correctly decides membership in $L_1 \cap L_2$ with (conditional) probability at least 2/3.

More generally, combinations of these ideas show that **PostBQP** is closed under union and BQP truth-table reductions.

PostBQP = PP

Scott Aaronson showed[5] that the complexity classes **PostBQP** (postselected bounded error quantum polynomial time) and **PP** (probabilistic polynomial time) are equal. The result was significant because this quantum computation reformulation of **PP** gave new insight and simpler proofs of properties of **PP**.

The usual definition of a **PostBQP** circuit family is one with two outbit qubits *P* (postselection) and *Q* (output) with a single measurement of *P* and *Q* at the end such that the probability of measuring $P = 1$ has nonzero probability, the conditional probability $\Pr[Q = 1|P = 1] \geq 2/3$ if the input *x* is in the language, and $\Pr[Q = 0|P = 1] \geq 2/3$ if the input *x* is not in the language. For technical reasons we tweak the definition of **PostBQP** as follows: we require that $\Pr[P = 1] \geq 2^{-n^c}$ for some constant *c* depending on the circuit family. Note this choice does not affect the basic properties of **PostBQP**, and also it can be shown that any computation consisting of typical gates (e.g. Hadamard, Toffoli) has this property whenever $\Pr[P = 1] > 0$.

Proving PostBQP ⊆ PP

Suppose we are given a **PostBQP** family of circuits to decide a language *L*. We assume without loss of generality (e.g. see the inessential properties of quantum computers) that all gates have transition matrices that are represented with real numbers, at the expense of adding one more qubit.

Let Ψ denote the final quantum state of the circuit before the postselecting measurement is made. The overall goal of the proof is to construct a **PP** algorithm to decide *L*. More specifically it suffices to have *L* correctly compare the squared amplitude of Ψ in the states with $Q = 1$, $P = 1$ to the squared amplitude

of Ψ in the states with $Q = 0$, $P = 1$ to determine which is bigger. The key insight is that the comparison of these amplitudes can be transformed into comparing the acceptance probability of a **PP** machine with 1/2.

Matrix view of PostBQP algorithms

Let *n* denote the input size, $B = B(n)$ denote the total number of qubits in the circuit (inputs, ancillary, output and postselection qubits), and $G = G(n)$ denote the total number of gates. Represent the *i*th gate by its transition matrix A^i (a real unitary $2^B \times 2^B$ matrix) and let the initial state be $|x\rangle$ (padded with zeroes). Then $\Psi = A^G A^{G-1} \cdots A^2 A^1 |x\rangle$. Define S_1 (resp. S_0) to be the set of basis states corresponding to $P = 1$, $Q = 1$ (resp. $P = 1$, $Q = 0$) and define the probabilities

$$\pi_1 := \Pr[P = 1, Q = 1] = \sum_{\omega \in S_1} \Psi_\omega^2$$

$$\pi_0 := \Pr[P = 1, Q = 0] = \sum_{\omega \in S_0} \Psi_\omega^2.$$

The definition of **PostBQP** ensures that either $\pi_1 \geq 2\pi_0$ or $\pi_0 \geq 2\pi_1$ according to whether *x* is in *L* or not.

Our **PP** machine will compare π_1 and π_0. In order to do this, we expand the definition of matrix multiplication:

$$\Psi_\omega = \sum_{\alpha_1, \ldots, \alpha_G} A^G_{\omega,\alpha_G} A^{G-1}_{\alpha_G,\alpha_{G-1}} \cdots A^2_{\alpha_3,\alpha_2} A^1_{\alpha_2,\alpha_1} x_{\alpha_1}$$

where the sum is taken over all lists of *G* basis vectors α_i. Now π_1 and π_0 can be expressed as a sum of pairwise products of these terms. Intuitively, we want to design a machine whose acceptance probability is something like $\frac{1}{2}(1 + \pi_1 - \pi_0)$, since then $x \in L$ would imply that the acceptance probability is $\frac{1}{2}(1 + \pi_1 - \pi_0) > \frac{1}{2}$, while $x \notin L$ would imply that the acceptance probability is $\frac{1}{2}(1 + \pi_1 - \pi_0) < \frac{1}{2}$.

Technicality: we may assume entries of the transition matrices A^i are rationals with denominator $2^{f(n)}$ for some polynomial *f*(*n*).

The definition of **PostBQP** tells us that $\pi_1 \geq \frac{2}{3}(\pi_0 + \pi_1)$ if *x* is in *L*, and that otherwise $\pi_0 \geq \frac{2}{3}(\pi_0 + \pi_1)$. Let us replace all entries of *A* by the nearest fraction with denominator $2^{f(n)}$ for a large polynomial $f(n)$ that we presently describe. What will be used later is that the *new* π values satisfy $\pi_1 > \frac{1}{2}(\pi_0 + \pi_1)$ if *x* is in *L*, and $\pi_0 > \frac{1}{2}(\pi_0 + \pi_1)$ if *x* is not in *L*. Using the earlier technical assumption and by analyzing how the 1-norm of the computational state changes, this is seen to be satisfied if $(1 + 2^{-f(n)} 2^B)^G - 1 < \frac{1}{6} 2^{-n^c}$, thus clearly there is a large enough *f* that is polynomial in *n*.

Constructing the PP machine

Now we provide the detailed implementation of our PP machine. Let α denote the sequence $\{\alpha_i\}_{i=1}^G$ and define the shorthand notation

$$\Pi(A,\omega,\alpha,x) := A^G_{\omega,\alpha_G} A^{G-1}_{\alpha_G,\alpha_{G-1}} \cdots A^2_{\alpha_3,\alpha_2} A^1_{\alpha_2,\alpha_1} x_{\alpha_1},$$

then

$$\pi_1 - \pi_0 = \sum_{\omega\in S_1}\sum_{\alpha,\alpha'} \Pi(A,\omega,\alpha,x)\Pi(A,\omega,\alpha',x) - \sum_{\omega\in S_0}\sum_{\alpha,\alpha'} \Pi(A,\omega,\alpha,x)\Pi(A,\omega,\alpha',x).$$

We define our PP machine to

- pick a basis state ω uniformly at random
- if $\omega \notin S_0 \cup S_1$ then STOP and accept with probability 1/2, reject with probability 1/2
- pick two sequences α, α' of G basis states uniformly at random
- compute $X = \Pi(A,\omega,\alpha,x)\Pi(A,\omega,\alpha',x)$ (which is a fraction with denominator $2^{2f(n)G(n)}$ such that $-1 \le X \le 1$)
- if $\omega \in S_1$ then accept with probability $\frac{1+X}{2}$ and reject with probability $\frac{1-X}{2}$ (which takes at most $2f(n)G(n)+1$ coin flips)
- otherwise (then $\omega \in S_0$) accept with probability $\frac{1-X}{2}$ and reject with probability $\frac{1+X}{2}$ (which again takes at most $2f(n)G(n)+1$ coin flips)

Then it is straightforward to compute that this machine accepts with probability $\frac{1}{2} + \frac{\pi_1-\pi_0}{2^{1+B(n)+2B(n)G(n)}}$, so this is a PP machine for the language L, as needed.

Proving PP ⊆ PostBQP

Suppose we have a PP machine with time complexity $T := T(n)$ on input x of length $n := |x|$. Thus the machine flips a coin at most T times during the computation. We can thus view the machine as a deterministic function f (implemented, e.g. by a classical circuit) which takes two inputs (x, r) where r, a binary string of length T, represents the results of the random coin flips that are performed by the computation, and the output of f is 1 (accept) or 0 (reject). The definition of PP tells us that

$$x \in L \Leftrightarrow \#\{r \in \{0,1\}^T \mid f(x,r) = 1\} > 2^{T-1}$$

Thus, we want a PostBQP algorithm that can determine whether the above statement is true.

Define s to be the number of random strings which lead to acceptance,

$$s := \#\{r \in \{0,1\}^T \mid f(x,r) = 1\}$$

and so $2^T - s$ is the number of rejected strings. It is straightforward to argue that without loss of generality, $s \notin \{0, 2^T/2, 2^T\}$; for details, see a similar without loss of generality assumption in the proof that **PP** is closed under complementation.

Aaronson's algorithm

Aaronson's algorithm for solving this problem is as follows. For simplicity, we will write all quantum states as unnormalized. First, we prepare the state $|x\rangle \otimes \sum_{r \in \{0,1\}^T} |r\rangle |f(x,r)\rangle$. Second, we apply Hadamard gates to the second register (each of the first *T* qubits), measure the second register and postselect on it being the all-zero string. It is easy to verify that this leaves the last register (the last qubit) in the residual state

$$|\psi\rangle := (2^T - s)|0\rangle + s|1\rangle.$$

Where *H* denotes the Hadamard gate, we compute the state

$$H|\psi\rangle = (2^T|0\rangle + (2^T - 2s)|1\rangle)/\sqrt{2}.$$

Where α, β are positive real numbers to be chosen later with $\alpha^2 + \beta^2 = 1$, we compute the state $\alpha|0\rangle|\psi\rangle + \beta|1\rangle|H\psi\rangle$ and measure the second qubit, postselecting on its value being equal to 1, which leaves the first qubit in a residual state depending on β/α which we denote

$$|\phi_{\beta/\alpha}\rangle := \alpha s|0\rangle + \frac{\beta}{\sqrt{2}}(2^T - 2s)|1\rangle.$$

Visualizing the possible states of a qubit as a circle, we see that if $s > 2^{T-1}$, (i.e. if $x \in L$) then $\phi_{\beta/\alpha}$ lies in the open quadrant $Q_{acc} := (-|1\rangle, |0\rangle)$ while if $s < 2^{T-1}$, (i.e. if $x \notin L$) then $\phi_{\beta/\alpha}$ lies in the open quadrant $Q_{rej} := (|0\rangle, |1\rangle)$. In fact for any fixed *x* (and its corresponding *s*), as we vary the ratio β/α in $(0, \infty)$, note that the image of $|\phi_{\beta/\alpha}\rangle$ is precisely the corresponding open quadrant. In the rest of the proof, we make precise the idea that we can distinguish between these two quadrants.

Analysis

Let $|+\rangle = (|1\rangle + |0\rangle)/\sqrt{2}$, which is the center of Q_{rej}, and let $|-\rangle$ be orthogonal to $|+\rangle$. Any qubit in Q_{acc}, when measured in the basis $\{|+\rangle, |-\rangle\}$, gives the value $|+\rangle$ less than 1/2 of the time. On the other hand, if $x \notin L$ and we had picked $\beta/\alpha = r^* := \sqrt{2}s/(2^T - 2s)$ then measuring $|\phi_{\beta/\alpha}\rangle$ in the basis $\{|+\rangle, |-\rangle\}$ would give the value $|+\rangle$ all of the time. Since we don't know *s* we also don't know the precise value of *r**, but we can try several (polynomially many) different values for β/α in hopes of getting one that is "near" *r**.

Specifically, note $2^{-T} < r* < 2^T$ and let us successively set β/α to every value of the form 2^i for $-T \leq i \leq T$. Then elementary calculations show that for one of these values of *i*, the probability that the measurement of $|\phi_{2^i}\rangle$ in the basis $\{|+\rangle, |-\rangle\}$ yields $|+\rangle$ is at least $(3 + 2\sqrt{2})/6 \approx 0.971$.

Overall, the **PostBQP** algorithm is as follows. Let *k* be any constant strictly between 1/2 and $(3+2\sqrt{2})/6$. We do the following experiment for each $-T \leq i \leq T$: construct and measure $|\phi_{2^i}\rangle$ in the basis $\{|+\rangle, |-\rangle\}$ a total of $C \log T$ times where *C* is a constant. If the proportion of $|+\rangle$ measurements is greater than *k*, then reject. If we don't reject for any *i*, accept. Chernoff bounds then show that for a sufficiently large universal constant *C*, we correctly classify *x* with probability at least 2/3.

Note that this algorithm satisfies the technical assumption that the overall postselection probability is not too small: each individual measurement of $|\phi_{2^i}\rangle$ has postselection probability $1/2^{O(T)}$ and so the overall probability is $1/2^{O(T^2 \log T)}$.

Implications

- See Quantum computation reformulation of **PP**

References

1. Y. Han and Hemaspaandra, L. and Thierauf, T. (1997). "Threshold computation and cryptographic security". *SIAM Journal on Computing*. **26**: 59–78. CiteSeerX 10.1.1.23.510 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.510). doi:10.1137/S0097539792240467 (https://doi.org/10.1137%2FS0097539792240467).
2. Aaronson, Scott (2005). "Quantum computing, postselection, and probabilistic polynomial-time". *Proceedings of the Royal Society A*. **461** (2063): 3473–3482. arXiv:quant-ph/0412187 (https://arxiv.org/abs/quant-ph/0412187). Bibcode:2005RSPSA.461.3473A (https://ui.adsabs.harvard.edu/abs/2005RSPSA.461.3473A). doi:10.1098/rspa.2005.1546 (https://doi.org/10.1098%2Frspa.2005.1546). S2CID 1770389 (https://api.semanticscholar.org/CorpusID:1770389).. Preprint available at [1] (https://arxiv.org/abs/quant-ph/0412187)
3. Aaronson, Scott (2004-01-11). "Complexity Class of the Week: PP" (http://weblog.fortnow.com/2004/01/complexity-class-of-week-pp-by-guest.html). *Computational Complexity Weblog*. Retrieved 2008-05-02.
4. Ethan Bernstein & Umesh Vazirani (1997). "Quantum Complexity Theory". *SIAM Journal on Computing*. **26** (5): 11–20. CiteSeerX 10.1.1.144.7852 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.144.7852). doi:10.1137/s0097539796300921 (https://doi.org/10.1137%2Fs0097539796300921).
5. Aaronson, Scott (2005). "Quantum computing, postselection, and probabilistic polynomial-time". *Proceedings of the Royal Society A*. **461** (2063): 3473–3482. arXiv:quant-ph/0412187 (https://arxiv.org/abs/quant-ph/0412187). Bibcode:2005RSPSA.461.3473A (https://ui.adsabs.harvard.edu/abs/2005RSPSA.461.3473A). doi:10.1098/rspa.2005.1546 (https://doi.org/10.1098%2Frspa.2005.1546). S2CID 1770389 (https://api.semanticscholar.org/CorpusID:1770389).

Retrieved from "https://en.wikipedia.org/w/index.php?title=PostBQP&oldid=1152403820"

WIKIPEDIA
The Free Encyclopedia

Quantum supremacy

In quantum computing, **quantum supremacy** or **quantum advantage** is the goal of demonstrating that a programmable quantum computer can solve a problem that no classical computer can solve in any feasible amount of time, irrespective of the usefulness of the problem.[1][2][3] The term was coined by John Preskill in 2012,[1][4] but the concept dates to Yuri Manin's 1980[5] and Richard Feynman's 1981[6] proposals of quantum computing.

Conceptually, quantum supremacy involves both the engineering task of building a powerful quantum computer and the computational-complexity-theoretic task of finding a problem that can be solved by that quantum computer and has a superpolynomial speedup over the best known or possible classical algorithm for that task.[7][8]

Examples of proposals to demonstrate quantum supremacy include the boson sampling proposal of Aaronson and Arkhipov,[9] and sampling the output of random quantum circuits.[10][11] The output distributions that are obtained by making measurements in boson sampling or quantum random circuit sampling are flat, but structured in a way so that one cannot classically efficiently sample from a distribution that is close to the distribution generated by the quantum experiment. For this conclusion to be valid, only very mild assumptions in the theory of computational complexity have to be invoked. In this sense, quantum random sampling schemes can have the potential to show quantum supremacy.[12]

A notable property of quantum supremacy is that it can be feasibly achieved by near-term quantum computers,[4] since it does not require a quantum computer to perform any useful task[13] or use high-quality quantum error correction,[14] both of which are long-term goals.[2] Consequently, researchers view quantum supremacy as primarily a scientific goal, with relatively little immediate bearing on the future commercial viability of quantum computing.[2] Due to unpredictable possible improvements in classical computers and algorithms, quantum supremacy may be temporary or unstable, placing possible achievements under significant scrutiny.[15][16]

Background

Quantum advantage in the 20th century

In 1936, Alan Turing published his paper, “On Computable Numbers”,[17] in response to the 1900 Hilbert Problems. Turing's paper described what he called a “universal computing machine”, which later became known as a Turing machine. In 1980, Paul Benioff used Turing's paper to propose the theoretical feasibility of Quantum Computing. His paper, “The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines“,[18] was the first to demonstrate that it is possible to show the reversible nature of quantum computing as long as the energy dissipated is arbitrarily small. In 1981, Richard Feynman showed that quantum mechanics could not be efficiently simulated on classical devices.[19] During a lecture, he delivered the famous quote, “Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it

quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."[19] Soon after this, David Deutsch produced a description for a quantum Turing machine and designed an algorithm created to run on a quantum computer.[20]

In 1994, further progress toward quantum supremacy was made when Peter Shor formulated Shor's algorithm, streamlining a method for factoring integers in polynomial time.[21] In 1995, Christopher Monroe and David Wineland published their paper, "Demonstration of a Fundamental Quantum Logic Gate",[22] marking the first demonstration of a quantum logic gate, specifically the two-bit "controlled-NOT". In 1996, Lov Grover put into motion an interest in fabricating a quantum computer after publishing his algorithm, Grover's Algorithm, in his paper, "A fast quantum mechanical algorithm for database search".[23] In 1998, Jonathan A. Jones and Michele Mosca published "Implementation of a Quantum Algorithm to Solve Deutsch's Problem on a Nuclear Magnetic Resonance Quantum Computer",[24] marking the first demonstration of a quantum algorithm.

Progress in the 21st century

Vast progress toward quantum supremacy was made in the 2000s from the first 5-qubit nuclear magnetic resonance computer (2000), the demonstration of Shor's theorem (2001), and the implementation of Deutsch's algorithm in a clustered quantum computer (2007).[25] In 2011, D-Wave Systems of Burnaby, British Columbia, Canada became the first company to sell a quantum computer commercially.[26] In 2012, physicist Nanyang Xu landed a milestone accomplishment by using an improved adiabatic factoring algorithm to factor 143. However, the methods used by Xu were met with objections.[27] Not long after this accomplishment, Google purchased its first quantum computer.[28]

Google had announced plans to demonstrate quantum supremacy before the end of 2017 with an array of 49 superconducting qubits.[29] In early January 2018, Intel announced a similar hardware program.[30] In October 2017, IBM demonstrated the simulation of 56 qubits on a classical supercomputer, thereby increasing the computational power needed to establish quantum supremacy.[31] In November 2018, Google announced a partnership with NASA that would "analyze results from quantum circuits run on Google quantum processors, and ... provide comparisons with classical simulation to both support Google in validating its hardware and establish a baseline for quantum supremacy."[32] Theoretical work published in 2018 suggested that quantum supremacy should be possible with a "two-dimensional lattice of 7×7 qubits and around 40 clock cycles" if error rates can be pushed low enough.[33] The scheme discussed was a variant of a quantum random sampling scheme in which qubits undergo random quantum circuits featuring quantum gates drawn from a universal gate set, followed by measurements in the computational basis.

On June 18, 2019, Quanta Magazine suggested that quantum supremacy could happen in 2019, according to Neven's law.[34] On September 20, 2019, the *Financial Times* reported that "Google claims to have reached quantum supremacy with an array of 54 qubits out of which 53 were functional, which were used to perform a series of operations in 200 seconds that would take a supercomputer about 10,000 years to complete".[35][36] On October 23, Google officially confirmed the claims.[37][38][39] IBM responded by suggesting some of the claims were excessive and suggested that it could take 2.5 days instead of 10,000 years, listing techniques that a classical supercomputer may use to maximize computing speed. IBM's response is relevant as the most powerful supercomputer at the time, Summit, was made by

IBM.[40][15][41] Researchers have since developed better algorithms for the sampling problem used to claim quantum supremacy, giving substantial reductions to the gap between Google's Sycamore processor and classical supercomputers[42][43][44] and even beating it.[45][46][47]

In December 2020, a group based in the University of Science and Technology of China (USTC) led by Jian-Wei Pan reached quantum supremacy by implementing gaussian boson sampling on 76 photons with their photonic quantum computer Jiuzhang.[48][49][50] The paper states that to generate the number of samples the quantum computer generates in 200 seconds, a classical supercomputer would require 2.5 billion years of computation.[3]

In October 2021, teams from USTC again reported quantum primacy by building two supercomputers called Jiuzhang 2.0 and Zuchongzhi. The light-based Jiuzhang 2.0 implemented gaussian boson sampling to detect 113 photons from a 144-mode optical interferometer and a sampling rate speed up of 10^{24} – a difference of 37 photons and 10 orders of magnitude over the previous Jiuzhang.[51][52] Zuchongzhi is a programmable superconducting quantum computer that needs to be kept at extremely low temperatures to work efficiently and uses random circuit sampling to obtain 56 qubits from a tunable coupling architecture of 66 transmons—an improvement over Google's Sycamore 2019 achievement by 3 qubits, meaning a greater computational cost of classical simulation of 2 to 3 orders of magnitude.[53][54][55] A third study reported that *Zuchongzhi 2.1* completed a sampling task that "is about 6 orders of magnitude more difficult than that of Sycamore" "in the classic simulation".[56]

In June 2022, Xanadu reported a boson sampling experiment summing to those of Google and USTC. Their setup used loops of optical fiber and multiplexing to replace the network of beam splitters by a single one which made it also more easily reconfigurable. They detected a mean of 125 up to 219 photons from 216 squeezed modes (squeezed light follows a photon number distribution so they can contain more than one photon per mode) and claim to have obtained a speedup 50 million times more than previous experiments.[57][58]

In March of 2024, D-Wave Systems reported on an experiment using a quantum annealing based processor that out-performed classical methods including tensor networks and neural networks. They argued that no known classical approach could yield the same results as the quantum simulation within a reasonable time-frame and claimed quantum supremacy. The task performed was the simulation of the non-equilibrium dynamics of a magnetic spin system quenched through a quantum phase transition.[59]

Computational complexity

Complexity arguments concern how the amount of some resource needed to solve a problem (generally time or memory) scales with the size of the input. In this setting, a *problem* consists of an inputted problem instance (a binary string) and returned solution (corresponding output string), while *resources* refers to designated elementary operations, memory usage, or communication. A collection of local operations allows for the computer to generate the output string. A circuit model and its corresponding operations are useful in describing both classical and quantum problems; the classical circuit model consists of basic operations such as AND gates, OR gates, and NOT gates while the quantum model consists of classical circuits and the application of unitary operations. Unlike the finite set of classical gates, there are an infinite amount of quantum gates due to the continuous nature of unitary operations. In both classical and quantum cases, complexity swells with increasing problem size.[60] As an extension of

classical computational complexity theory, quantum complexity theory considers what a theoretical universal quantum computer could accomplish without accounting for the difficulty of building a physical quantum computer or dealing with decoherence and noise.[61] Since quantum information is a generalization of classical information, quantum computers can simulate any classical algorithm.[61]

Quantum complexity classes are sets of problems that share a common quantum computational model, with each model containing specified resource constraints. Circuit models are useful in describing quantum complexity classes.[62] The most useful quantum complexity class is BQP (bounded-error quantum polynomial time), the class of decision problems that can be solved in polynomial time by a universal quantum computer. Questions about BQP still remain, such as the connection between BQP and the polynomial-time hierarchy, whether or not BQP contains NP-complete problems, and the exact lower and upper bounds of the BQP class. Not only would answers to these questions reveal the nature of BQP, but they would also answer difficult classical complexity theory questions. One strategy for better understanding BQP is by defining related classes, ordering them into a conventional class hierarchy, and then looking for properties that are revealed by their relation to BQP.[63] There are several other quantum complexity classes, such as QMA (quantum Merlin Arthur) and QIP (quantum interactive polynomial time).[62]

The difficulty of proving what cannot be done with classical computing is a common problem in definitively demonstrating quantum supremacy. Contrary to decision problems that require yes or no answers, sampling problems ask for samples from probability distributions.[64] If there is a classical algorithm that can efficiently sample from the output of an arbitrary quantum circuit, the polynomial hierarchy would collapse to the third level, which is generally considered to be very unlikely.[10][11] Boson sampling is a more specific proposal, the classical hardness of which depends upon the intractability of calculating the permanent of a large matrix with complex entries, which is a #P-complete problem.[65] The arguments used to reach this conclusion have been extended to IQP Sampling,[66] where only the conjecture that the average- and worst-case complexities of the problem are the same is needed,[64] as well as to Random Circuit Sampling,[11] which is the task replicated by the Google[38] and USTC research groups.[48]

Proposed experiments

The following are proposals for demonstrating quantum computational supremacy using current technology, often called NISQ devices.[2] Such proposals include (1) a well-defined computational problem, (2) a quantum algorithm to solve this problem, (3) a comparison best-case classical algorithm to solve the problem, and (4) a complexity-theoretic argument that, under a reasonable assumption, no classical algorithm can perform significantly better than current algorithms (so the quantum algorithm still provides a superpolynomial speedup).[7][67]

Shor's algorithm for factoring integers

This algorithm finds the prime factorization of an *n*-bit integer in $\tilde{O}(n^3)$ time[68] whereas the best known classical algorithm requires $2^{O(n^{1/3})}$ time and the best upper bound for the complexity of this problem is $O(2^{n/3+o(1)})$.[69] It can also provide a speedup for any problem that reduces to integer factoring, including the membership problem for matrix groups over fields of odd order.[70]

This algorithm is important both practically and historically for quantum computing. It was the first polynomial-time quantum algorithm proposed for a real-world problem that is believed to be hard for classical computers.[68] Namely, it gives a superpolynomial speedup under the reasonable assumption that RSA, a well-established cryptosystem, is secure.[71]

Factoring has some benefit over other supremacy proposals because factoring can be *checked* quickly with a classical computer just by multiplying integers, even for large instances where factoring algorithms are intractably slow. However, implementing Shor's algorithm for large numbers is infeasible with current technology,[72][73] so it is not being pursued as a strategy for demonstrating supremacy.

Boson sampling

This computing paradigm based upon sending identical photons through a linear-optical network can solve certain sampling and search problems that, assuming a few complexity-theoretical conjectures (that calculating the permanent of Gaussian matrices is #P-Hard and that the polynomial hierarchy does not collapse) are intractable for classical computers.[9] However, it has been shown that boson sampling in a system with large enough loss and noise can be simulated efficiently.[74]

The largest experimental implementation of boson sampling to date had 6 modes so could handle up to 6 photons at a time.[75] The best proposed classical algorithm for simulating boson sampling runs in time $O(n2^n + mn^2)$ for a system with *n* photons and *m* output modes.[76][77] BosonSampling (https://CRAN.R-project.org/package=BosonSampling) is an open-source implementation in the R programming language. The algorithm leads to an estimate of 50 photons required to demonstrate quantum supremacy with boson sampling.[76][77]

Sampling the output distribution of random quantum circuits

The best known algorithm for simulating an arbitrary random quantum circuit requires an amount of time that scales exponentially with the number of qubits, leading one group to estimate that around 50 qubits could be enough to demonstrate quantum supremacy.[33] Bouland, Fefferman, Nirkhe and Vazirani[11] gave, in 2018, theoretical evidence that efficiently simulating a random quantum circuit would require a collapse of the computational polynomial hierarchy. Google had announced its intention to demonstrate quantum supremacy by the end of 2017 by constructing and running a 49-qubit chip that would be able to sample distributions inaccessible to any current classical computers in a reasonable amount of time.[29] The largest universal quantum circuit simulator running on classical supercomputers at the time was able to simulate 48 qubits.[78] But for particular kinds of circuits, larger quantum circuit simulations with 56 qubits are possible.[79] This may require increasing the number of qubits to demonstrate quantum supremacy.[31] On October 23, 2019, Google published the results of this quantum supremacy experiment in the Nature article, “Quantum Supremacy Using a Programmable Superconducting Processor” in which they developed a new 53-qubit processor, named “Sycamore”, that is capable of fast, high-fidelity quantum logic gates, in order to perform the benchmark testing. Google claims that their machine performed the target computation in 200 seconds, and estimated that their classical algorithm would take

10,000 years in the world's fastest supercomputer to solve the same problem.[80] IBM disputed this claim, saying that an improved classical algorithm should be able to solve that problem in two and a half days on that same supercomputer.[81][82][83]

Criticisms

Susceptibility to error

Quantum computers are much more susceptible to errors than classical computers due to decoherence and noise.[84] The threshold theorem states that a noisy quantum computer can use quantum error-correcting codes[85][86] to simulate a noiseless quantum computer, assuming the error introduced in each computer cycle is less than some number.[87] Numerical simulations suggest that that number may be as high as 3%.[88] However, it is not yet definitively known how the resources needed for error correction will scale with the number of qubits.[89] Skeptics point to the unknown behavior of noise in scaled-up quantum systems as a potential roadblock for successfully implementing quantum computing and demonstrating quantum supremacy.[84][90]

Criticism of the name

Some researchers have suggested that the term "quantum supremacy" should not be used, arguing that the word "supremacy" evokes distasteful comparisons to the racist belief of white supremacy. A controversial[91][92] commentary article in the journal *Nature* signed by thirteen researchers asserts that the alternative phrase "quantum advantage" should be used instead.[93] John Preskill, the professor of theoretical physics at the California Institute of Technology who coined the term, has since clarified that the term was proposed to explicitly describe the moment that a quantum computer gains the ability to perform a task that a classical computer never could. He further explained that he specifically rejected the term "quantum advantage" as it did not fully encapsulate the meaning of his new term: the word "advantage" would imply that a computer with quantum supremacy would have a slight edge over a classical computer while the word "supremacy" better conveys complete ascendancy over any classical computer.[4] *Nature's* Philip Ball wrote in December 2020 that the term "quantum advantage" has "largely replaced" the term "quantum supremacy".[94]

See also

- Gottesman–Knill theorem
- List of quantum processors
  - Sycamore processor
  - Jiuzhang (quantum computer)
- Noisy intermediate-scale quantum era

References

1. Preskill, John (2012-03-26). "Quantum computing and the entanglement frontier".

arXiv:1203.5813 (https://arxiv.org/abs/1203.5813) [quant-ph (https://arxiv.org/archive/quant-ph)].

2. Preskill, John (2018-08-06). "Quantum Computing in the NISQ era and beyond" (https://doi.org/10.22331%2Fq-2018-08-06-79). *Quantum*. **2**: 79. arXiv:1801.00862 (https://arxiv.org/abs/1801.00862). Bibcode:2018Quant...2...79P (https://ui.adsabs.harvard.edu/abs/2018Quant...2...79P). doi:10.22331/q-2018-08-06-79 (https://doi.org/10.22331%2Fq-2018-08-06-79).
3. Zhong, Han-Sen; Wang, Hui; Deng, Yu-Hao; Chen, Ming-Cheng; Peng, Li-Chao; Luo, Yi-Han; Qin, Jian; Wu, Dian; Ding, Xing; Hu, Yi; Hu, Peng (2020-12-03). "Quantum computational advantage using photons" (https://www.science.org/doi/10.1126/science.abe8770). *Science*. **370** (6523): 1460–1463. arXiv:2012.01625 (https://arxiv.org/abs/2012.01625). Bibcode:2020Sci...370.1460Z (https://ui.adsabs.harvard.edu/abs/2020Sci...370.1460Z). doi:10.1126/science.abe8770 (https://doi.org/10.1126%2Fscience.abe8770). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 33273064 (https://pubmed.ncbi.nlm.nih.gov/33273064). S2CID 227254333 (https://api.semanticscholar.org/CorpusID:227254333).
4. "John Preskill Explains 'Quantum Supremacy' " (https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/). *Quanta Magazine*. 2 October 2019. Retrieved 2020-04-21.
5. Manin, Yu. I. (1980). *Vychislimoe i nevychislimoe* (https://web.archive.org/web/20130510173823/http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) [*Computable and Noncomputable*] (in Russian). Sov.Radio. pp. 13–15. Archived from the original (http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5Bdjv%5D.zip) on 2013-05-10. Retrieved 2013-03-04.
6. Feynman, Richard P. (1982-06-01). "Simulating Physics with Computers". *International Journal of Theoretical Physics*. **21** (6–7): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). CiteSeerX 10.1.1.45.9310 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.9310). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). ISSN 0020-7748 (https://search.worldcat.org/issn/0020-7748). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445).
7. Harrow, Aram W.; Montanaro, Ashley (September 2017). "Quantum computational supremacy". *Nature*. **549** (7671): 203–209. arXiv:1809.07442 (https://arxiv.org/abs/1809.07442). Bibcode:2017Natur.549..203H (https://ui.adsabs.harvard.edu/abs/2017Natur.549..203H). doi:10.1038/nature23458 (https://doi.org/10.1038%2Fnature23458). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 28905912 (https://pubmed.ncbi.nlm.nih.gov/28905912). S2CID 2514901 (https://api.semanticscholar.org/CorpusID:2514901).
8. Papageorgiou, Anargyros; Traub, Joseph F. (2013-08-12). "Measures of quantum computing speedup". *Physical Review A*. **88** (2): 022316. arXiv:1307.7488 (https://arxiv.org/abs/1307.7488). Bibcode:2013PhRvA..88b2316P (https://ui.adsabs.harvard.edu/abs/2013PhRvA..88b2316P). doi:10.1103/PhysRevA.88.022316 (https://doi.org/10.1103%2FPhysRevA.88.022316). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 41867048 (https://api.semanticscholar.org/CorpusID:41867048).
9. Aaronson, Scott; Arkhipov, Alex (2011). "The computational complexity of linear optics". *Proceedings of the forty-third annual ACM symposium on Theory of computing*. STOC '11. New York, New York, United States: Association for Computing Machinery. pp. 333–342. arXiv:1011.3245 (https://arxiv.org/abs/1011.3245). doi:10.1145/1993636.1993682 (https://doi.org/10.1145%2F1993636.1993682). ISBN 9781450306911. S2CID 681637 (https://api.semanticscholar.org/CorpusID:681637).
10. Aaronson, Scott; Chen, Lijie (2016-12-18). "Complexity-Theoretic Foundations of Quantum Supremacy Experiments". arXiv:1612.05903 (https://arxiv.org/abs/1612.05903) [quant-ph (https://arxiv.org/archive/quant-ph)].

11. Bouland, Adam; Fefferman, Bill; Nirkhe, Chinmay; Vazirani, Umesh (2018-10-29). "On the complexity and verification of quantum random circuit sampling" (https://dx.doi.org/10.1038/s41567-018-0318-2). *Nature Physics*. **15** (2): 159–163. arXiv:1803.04402 (https://arxiv.org/abs/1803.04402). doi:10.1038/s41567-018-0318-2 (https://doi.org/10.1038%2Fs41567-018-0318-2). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 125264133 (https://api.semanticscholar.org/CorpusID:125264133).
12. Hangleiter, Dominik; Eisert, Jens (2023-07-20). "Computational advantage of quantum random sampling". *Reviews of Modern Physics*. **95** (3): 035001. arXiv:2206.04079 (https://arxiv.org/abs/2206.04079). Bibcode:2023RvMP...95c5001H (https://ui.adsabs.harvard.edu/abs/2023RvMP...95c5001H). doi:10.1103/RevModPhys.95.035001 (https://doi.org/10.1103%2FRevModPhys.95.035001). S2CID 249538723 (https://api.semanticscholar.org/CorpusID:249538723).
13. Metz, Cade (2019-10-23). "Google Claims a Quantum Breakthrough That Could Change Computing (Published 2019)" (https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html). *The New York Times*. ISSN 0362-4331 (https://search.worldcat.org/issn/0362-4331). Retrieved 2020-12-07.
14. Aaronson, Scott (2019-10-30). "Opinion | Why Google's Quantum Supremacy Milestone Matters (Published 2019)" (https://www.nytimes.com/2019/10/30/opinion/google-quantum-computer-sycamore.html). *The New York Times*. ISSN 0362-4331 (https://search.worldcat.org/issn/0362-4331). Retrieved 2020-12-07.
15. "On "Quantum Supremacy" " (https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/). *IBM Research Blog*. 2019-10-22. Retrieved 2019-10-24.
16. Crane, Leah. "IBM says Google may not have reached quantum supremacy after all" (https://www.newscientist.com/article/2220813-ibm-says-google-may-not-have-reached-quantum-supremacy-after-all/). *New Scientist*. Retrieved 2020-12-07.
17. Turing, Alan (1936). *On Computable Numbers, With An Application To The Entscheidungsproblem*.
18. Benioff, Paul (1980-05-01). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines" (https://doi.org/10.1007/BF01011339). *Journal of Statistical Physics*. **22** (5): 563–591. Bibcode:1980JSP....22..563B (https://ui.adsabs.harvard.edu/abs/1980JSP....22..563B). doi:10.1007/BF01011339 (https://doi.org/10.1007%2FBF01011339). ISSN 1572-9613 (https://search.worldcat.org/issn/1572-9613). S2CID 122949592 (https://api.semanticscholar.org/CorpusID:122949592).
19. Feynman, Richard P. (1982-06-01). "Simulating physics with computers" (https://doi.org/10.1007/BF02650179). *International Journal of Theoretical Physics*. **21** (6): 467–488. Bibcode:1982IJTP...21..467F (https://ui.adsabs.harvard.edu/abs/1982IJTP...21..467F). doi:10.1007/BF02650179 (https://doi.org/10.1007%2FBF02650179). ISSN 1572-9575 (https://search.worldcat.org/issn/1572-9575). S2CID 124545445 (https://api.semanticscholar.org/CorpusID:124545445).
20. "Quantum Computing" (https://plato.stanford.edu/entries/qt-quantcomp/). *Stanford Encyclopedia of Philosophy*. September 30, 2019.
21. Shor, Peter (1996). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*.
22. Monroe, C.; Meekhof, D. M.; King, B. E.; Itano, W. M.; Wineland, D. J. (1995-12-18). "Demonstration of a Fundamental Quantum Logic Gate" (https://doi.org/10.1103%2FPhysRevLett.75.4714). *Physical Review Letters*. **75** (25): 4714–4717. Bibcode:1995PhRvL..75.4714M (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75.4714M). doi:10.1103/PhysRevLett.75.4714 (https://doi.org/10.1103%2FPhysRevLett.75.4714). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10059979 (https://pubmed.ncbi.nlm.nih.gov/10059979).

23. Grover, Lov K. (1996-11-19). "A fast quantum mechanical algorithm for database search". arXiv:quant-ph/9605043 (https://arxiv.org/abs/quant-ph/9605043).
24. Jones, J. A.; Mosca, M. (August 1998). "Implementation of a Quantum Algorithm to Solve Deutsch's Problem on a Nuclear Magnetic Resonance Quantum Computer". *The Journal of Chemical Physics*. **109** (5): 1648–1653. arXiv:quant-ph/9801027 (https://arxiv.org/abs/quant-ph/9801027). doi:10.1063/1.476739 (https://doi.org/10.1063%2F1.476739). ISSN 0021-9606 (https://search.worldcat.org/issn/0021-9606). S2CID 19348964 (https://api.semanticscholar.org/CorpusID:19348964).
25. Balaganur, Sameer (2019-11-20). "Man's Race To Quantum Supremacy: The Complete Timeline" (https://analyticsindiamag.com/race-quantum-supremacy-complete-timeline/). *Analytics India Magazine*. Retrieved 2020-11-16.
26. Merali, Zeeya (June 2011). "First sale for quantum computing" (https://doi.org/10.1038%2F474018a). *Nature*. **474** (7349): 18. Bibcode:2011Natur.474...18M (https://ui.adsabs.harvard.edu/abs/2011Natur.474...18M). doi:10.1038/474018a (https://doi.org/10.1038%2F474018a). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 21637232 (https://pubmed.ncbi.nlm.nih.gov/21637232). S2CID 4425833 (https://api.semanticscholar.org/CorpusID:4425833).
27. Battersby, Stephen (13 April 2012). "Controversial quantum computer beats factoring record" (https://www.newscientist.com/article/dn21699-controversial-quantum-computer-beats-factoring-record/). *New Scientist*. Retrieved 2020-11-16.
28. Hardy, Quentin (2013-05-16). "Google Buys a Quantum Computer" (https://bits.blogs.nytimes.com/2013/05/16/google-buys-a-quantum-computer/). *Bits Blog*. Retrieved 2020-11-16.
29. Courtland, Rachel (24 May 2017). "Google Plans to Demonstrate the Supremacy of Quantum Computing" (https://spectrum.ieee.org/google-plans-to-demonstrate-the-supremacy-of-quantum-computing). *IEEE Spectrum*. Retrieved 2018-01-11.
30. Hsu, Jeremy (8 January 2018). "CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy" (https://spectrum.ieee.org/intels-49qubit-chip-aims-for-quantum-supremacy). *IEEE Spectrum*. Retrieved 2017-07-22.
31. Kim, Mark (October 20, 2017). "Google's quantum computing plans threatened by IBM curveball" (https://www.newscientist.com/article/2151032-googles-quantum-computing-plans-threatened-by-ibm-curveball/). *New Scientist*. Retrieved October 22, 2017.
32. Harris, Mark (November 5, 2018). "Google has enlisted NASA to help it prove quantum supremacy within months" (https://www.technologyreview.com/s/612381/google-has-enlisted-nasa-to-help-it-prove-quantum-supremacy-within-months/). *MIT Technology Review*. Retrieved 2018-11-30.
33. Boixo, Sergio; Isakov, Sergei V.; Smelyanskiy, Vadim N.; Babbush, Ryan; Ding, Nan; Jiang, Zhang; Bremner, Michael J.; Martinis, John M.; Neven, Hartmut (23 April 2018). "Characterizing quantum supremacy in near-term devices". *Nature Physics*. **14** (6): 595–600. arXiv:1608.00263 (https://arxiv.org/abs/1608.00263). Bibcode:2018NatPh..14..595B (https://ui.adsabs.harvard.edu/abs/2018NatPh..14..595B). doi:10.1038/s41567-018-0124-x (https://doi.org/10.1038%2Fs41567-018-0124-x). S2CID 4167494 (https://api.semanticscholar.org/CorpusID:4167494).
34. Hartnett, Kevin (June 18, 2019). "A New Law to Describe Quantum Computing's Rise?" (https://www.quantamagazine.org/does-nevens-law-describe-quantum-computings-rise-20190618/). *Quanta Magazine*.
35. [1] (https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17), *Financial Times*, September 2019 (subscription required)
36. "Google touts quantum computing milestone" (https://www.marketwatch.com/story/google-touts-quantum-computing-milestone-2019-10-23). *MarketWatch*. Associated Press.
37. "Demonstrating Quantum Supremacy" (https://www.youtube.com/watch?v=-ZNEzzDcllU) – via www.youtube.com.

38. "Quantum Supremacy Using a Programmable Superconducting Processor" (http://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html).
39. Arute, Frank; et al. (23 October 2019). "Quantum supremacy using a programmable superconducting processor" (https://doi.org/10.1038%2Fs41586-019-1666-5). *Nature*. **574** (7779): 505–510. arXiv:1910.11333 (https://arxiv.org/abs/1910.11333). Bibcode:2019Natur.574..505A (https://ui.adsabs.harvard.edu/abs/2019Natur.574..505A). doi:10.1038/s41586-019-1666-5 (https://doi.org/10.1038%2Fs41586-019-1666-5). PMID 31645734 (https://pubmed.ncbi.nlm.nih.gov/31645734).
40. "What the Google vs. IBM debate over quantum supremacy means" (https://www.zdnet.com/article/what-the-google-v-ibm-debate-over-quantum-means/). *ZDNet*.
41. Zialcita, Paolo (23 October 2019). "Google Claims To Achieve Quantum Supremacy — IBM Pushes Back" (https://www.npr.org/2019/10/23/772710977/google-claims-to-achieve-quantum-supremacy-ibm-pushes-back). *NPR*. Retrieved 2019-10-24.
42. Liu, Yong (Alexander); Liu, Xin (Lucy); Li, Fang (Nancy); Fu, Haohuan; Yang, Yuling; Song, Jiawei; Zhao, Pengpeng; Wang, Zhen; Peng, Dajia; Chen, Huarong; Guo, Chu (2021-11-14). "Closing the "quantum supremacy" gap" (https://doi.org/10.1145/3458817.3487399). *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*. SC '21. New York, New York, United States: Association for Computing Machinery. pp. 1–12. arXiv:2110.14502 (https://arxiv.org/abs/2110.14502). doi:10.1145/3458817.3487399 (https://doi.org/10.1145%2F3458817.3487399). ISBN 978-1-4503-8442-1. S2CID 239036985 (https://api.semanticscholar.org/CorpusID:239036985).
43. Bulmer, Jacob F. F.; Bell, Bryn A.; Chadwick, Rachel S.; Jones, Alex E.; Moise, Diana; Rigazzi, Alessandro; Thorbecke, Jan; Haus, Utz-Uwe; Van Vaerenbergh, Thomas; Patel, Raj B.; Walmsley, Ian A. (2022-01-28). "The boundary for quantum advantage in Gaussian boson sampling" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8791606). *Science Advances*. **8** (4): eabl9236. arXiv:2108.01622 (https://arxiv.org/abs/2108.01622). Bibcode:2022SciA....8.9236B (https://ui.adsabs.harvard.edu/abs/2022SciA....8.9236B). doi:10.1126/sciadv.abl9236 (https://doi.org/10.1126%2Fsciadv.abl9236). ISSN 2375-2548 (https://search.worldcat.org/issn/2375-2548). PMC 8791606 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8791606). PMID 35080972 (https://pubmed.ncbi.nlm.nih.gov/35080972).
44. McCormick, Katie (2022-02-10). "Race Not Over Between Classical and Quantum Computers" (https://physics.aps.org/articles/v15/19). *Physics*. **15**: 19. Bibcode:2022PhyOJ..15...19M (https://ui.adsabs.harvard.edu/abs/2022PhyOJ..15...19M). doi:10.1103/Physics.15.19 (https://doi.org/10.1103%2FPhysics.15.19). S2CID 246910085 (https://api.semanticscholar.org/CorpusID:246910085).
45. Pan, Feng; Chen, Keyang; Zhang, Pan (2022). "Solving the Sampling Problem of the Sycamore Quantum Circuits" (https://journals.aps.org/prl/accepted/f9079Kc7Yd613a0ec6447153516a99a03ca737793). *Physical Review Letters*. **129** (9): 090502. arXiv:2111.03011 (https://arxiv.org/abs/2111.03011). Bibcode:2022PhRvL.129i0502P (https://ui.adsabs.harvard.edu/abs/2022PhRvL.129i0502P). doi:10.1103/PhysRevLett.129.090502 (https://doi.org/10.1103%2FPhysRevLett.129.090502). PMID 36083655 (https://pubmed.ncbi.nlm.nih.gov/36083655). S2CID 251755796 (https://api.semanticscholar.org/CorpusID:251755796).
46. "Ordinary computers can beat Google's quantum computer after all" (https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all). 2022-08-02. doi:10.1126/science.ade2364 (https://doi.org/10.1126%2Fscience.ade2364). `{{cite journal}}`: Cite journal requires `|journal=` (help)
47. "Google's 'quantum supremacy' usurped by researchers using ordinary supercomputer" (https://techcrunch.com/2022/08/05/googles-quantum-supremacy-usurped-by-researchers-using-ordinary-supercomputer/). *TechCrunch*. Retrieved 2022-08-07.
48. Ball, Philip (2020-12-03). "Physicists in China challenge Google's 'quantum advantage' ". *Nature*. **588** (7838): 380. Bibcode:2020Natur.588..380B (https://ui.adsabs.harvard.edu/abs/2020Natur.588..380B). doi:10.1038/d41586-020-03434-7 (https://doi.org/10.1038%2Fd41586-020-03434-7). PMID 33273711 (https://pubmed.ncbi.nlm.nih.gov/33273711).

49. Garisto, Daniel (December 3, 2020). "Light-based Quantum Computer Exceeds Fastest Classical Supercomputers" (https://www.scientificamerican.com/article/light-based-quantum-computer-exceeds-fastest-classical-supercomputers/). *Scientific American*. Retrieved 2020-12-07.
50. Conover, Emily (2020-12-03). "The new light-based quantum computer Jiuzhang has achieved quantum supremacy" (https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy). *Science News*. Retrieved 2020-12-07.
51. Zhong, Han-Sen; Deng, Yu-Hao; Qin, Jian; Wang, Hui; Chen, Ming-Cheng; Peng, Li-Chao; Luo, Yi-Han; Wu, Dian; Gong, Si-Qiu; Su, Hao; Hu, Yi (2021-10-25). "Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light" (https://link.aps.org/doi/10.1103/PhysRevLett.127.180502). *Physical Review Letters*. **127** (18): 180502. arXiv:2106.15534 (https://arxiv.org/abs/2106.15534). Bibcode:2021PhRvL.127r0502Z (https://ui.adsabs.harvard.edu/abs/2021PhRvL.127r0502Z). doi:10.1103/PhysRevLett.127.180502 (https://doi.org/10.1103%2FPhysRevLett.127.180502). PMID 34767431 (https://pubmed.ncbi.nlm.nih.gov/34767431). S2CID 235669908 (https://api.semanticscholar.org/CorpusID:235669908).
52. Johnston, Hamish (26 October 2021). "Quantum advantage takes a giant leap in optical and superconducting systems" (https://physicsworld.com/quantum-advantage-takes-a-giant-leap-in-optical-and-superconducting-systems/). *Physics World*. Retrieved 2021-10-27.
53. Wu, Yulin; Bao, Wan-Su; Cao, Sirui; Chen, Fusheng; Chen, Ming-Cheng; Chen, Xiawei; Chung, Tung-Hsun; Deng, Hui; Du, Yajie; Fan, Daojin; Gong, Ming (2021-10-25). "Strong Quantum Computational Advantage Using a Superconducting Quantum Processor" (https://link.aps.org/doi/10.1103/PhysRevLett.127.180501). *Physical Review Letters*. **127** (18): 180501. arXiv:2106.14734 (https://arxiv.org/abs/2106.14734). Bibcode:2021PhRvL.127r0501W (https://ui.adsabs.harvard.edu/abs/2021PhRvL.127r0501W). doi:10.1103/PhysRevLett.127.180501 (https://doi.org/10.1103%2FPhysRevLett.127.180501). PMID 34767433 (https://pubmed.ncbi.nlm.nih.gov/34767433). S2CID 235658633 (https://api.semanticscholar.org/CorpusID:235658633).
54. Zhong, Han-Sen; Deng, Yu-Hao; Qin, Jian; Wang, Hui; Chen, Ming-Cheng; Peng, Li-Chao; Luo, Yi-Han; Wu, Dian; Gong, Si-Qiu; Su, Hao; Hu, Yi; Hu, Peng; Yang, Xiao-Yan; Zhang, Wei-Jun; Li, Hao; Li, Yuxuan; Jiang, Xiao; Gan, Lin; Yang, Guangwen; You, Lixing; Wang, Zhen; Li, Li; Liu, Nai-Le; Renema, Jelmer J.; Lu, Chao-Yang; Pan, Jian-Wei (25 October 2021). "Phase-Programmable Gaussian Boson Sampling Using Stimulated Squeezed Light". *Physical Review Letters*. **127** (18): 180502. arXiv:2106.15534 (https://arxiv.org/abs/2106.15534). Bibcode:2021PhRvL.127r0502Z (https://ui.adsabs.harvard.edu/abs/2021PhRvL.127r0502Z). doi:10.1103/PhysRevLett.127.180502 (https://doi.org/10.1103%2FPhysRevLett.127.180502). PMID 34767431 (https://pubmed.ncbi.nlm.nih.gov/34767431). S2CID 235669908 (https://api.semanticscholar.org/CorpusID:235669908).
55. Sanders, Barry C. (2021-10-25). "Quantum Leap for Quantum Primacy" (https://physics.aps.org/articles/v14/147). *Physics*. **14**: 147. Bibcode:2021PhyOJ..14..147S (https://ui.adsabs.harvard.edu/abs/2021PhyOJ..14..147S). doi:10.1103/Physics.14.147 (https://doi.org/10.1103%2FPhysics.14.147). S2CID 244826882 (https://api.semanticscholar.org/CorpusID:244826882).
56. Qingling Zhu, Sirui Cao; et al. (25 October 2021). "Quantum computational advantage via 60-qubit 24-cycle random circuit sampling". *Science Bulletin*. **67** (3): 240–245. arXiv:2109.03494 (https://arxiv.org/abs/2109.03494). doi:10.1016/j.scib.2021.10.017 (https://doi.org/10.1016%2Fj.scib.2021.10.017). ISSN 2095-9273 (https://search.worldcat.org/issn/2095-9273). PMID 36546072 (https://pubmed.ncbi.nlm.nih.gov/36546072). S2CID 237442167 (https://api.semanticscholar.org/CorpusID:237442167).

57. Brod, Daniel Jost (1 June 2022). "Loops simplify a set-up to boost quantum computational advantage" (https://www.nature.com/articles/d41586-022-01402-x). *Nature*. **606** (7912): 31–32. Bibcode:2022Natur.606...31B (https://ui.adsabs.harvard.edu/abs/2022Natur.606...31B). doi:10.1038/d41586-022-01402-x (https://doi.org/10.1038%2Fd41586-022-01402-x). PMID 35650360 (https://pubmed.ncbi.nlm.nih.gov/35650360). S2CID 249277681 (https://api.semanticscholar.org/CorpusID:249277681).
58. Madsen, Lars S.; Laudenbach, Fabian; Askarani, Mohsen Falamarzi; Rortais, Fabien; Vincent, Trevor; Bulmer, Jacob F. F.; Miatto, Filippo M.; Neuhaus, Leonhard; Helt, Lukas G.; Collins, Matthew J.; Lita, Adriana E. (1 June 2022). "Quantum computational advantage with a programmable photonic processor" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9159949). *Nature*. **606** (7912): 75–81. Bibcode:2022Natur.606...75M (https://ui.adsabs.harvard.edu/abs/2022Natur.606...75M). doi:10.1038/s41586-022-04725-x (https://doi.org/10.1038%2Fs41586-022-04725-x). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9159949 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9159949). PMID 35650354 (https://pubmed.ncbi.nlm.nih.gov/35650354).
59. King, Andrew; Nocera, Alberto; Rams, Marek; Dziarmaga, Jacek; Wiersema, Roeland; Bernoudy, William; Raymond, Jack; Kaushal, Nitin; Heinsdorf, Niclas; Harris, Richard; Boothby, Kelly; Altomare, Fabio; Berkley, Andrew; Boschnak, Martin; Chern, Kevin; Christiani, Holly; Cibere, Samantha; Connor, Jake; Dehn, Martin; Deshpande, Rahul; Ejtemaee, Sara; Farré, Pau; Hamer, Kelsey; Hoskinson, Emile; Huang, Shuiyuan; Johnson, Mark; Kortas, Samuel; Ladizinsky, Eric; Lai, Tony; Lanting, Trevor; Li, Ryan; MacDonald, Allison; Marsden, Gaelen; McGeoch, Catherine; Molavi, Reza; Neufeld, Richard; Norouzpour, Mana; Oh, Travis; Pasvolsky, Joel; Poitras, Patrick; Poulin-Lamarre, Gabriel; Prescott, Thomas; Reis, Mauricio; Rich, Chris; Samani, Mohammad; Sheldan, Benjamin; Smirnov, Anatoly; Sterpka, Edward; Trullas Clavera, Berta; Tsai, Nicholas; Volkmann, Mark; Whiticar, Alexander; Whittaker, Jed; Wilkinson, Warren; Yao, Jason; Yi, T.J.; Sandvik, Anders; Alvarez, Gonzalo; Melko, Roger; Carrasquilla, Juan; Franz, Marcel; Amin, Mohammad (1 March 2024). "Computational supremacy in quantum simulation". arXiv:2403.00910v1 (https://arxiv.org/abs/2403.00910v1).
60. Cleve, Richard (2000). "An Introduction to Quantum Complexity Theory" (https://cds.cern.ch/record/392006/files/9906111.pdf) (PDF). *CERN*. Bibcode:2000qcqi.book..103C (https://ui.adsabs.harvard.edu/abs/2000qcqi.book..103C).
61. Watrous, John (2009). "Quantum Computational Complexity". In Meyers, Robert A. (ed.). *Encyclopedia of Complexity and Systems Science* (https://archive.org/details/encyclopediacomp00meye). Springer New York. pp. 7174 (https://archive.org/details/encyclopediacomp00meye/page/n3382)–7201. doi:10.1007/978-0-387-30440-3_428 (https://doi.org/10.1007%2F978-0-387-30440-3_428). ISBN 9780387758886. S2CID 1380135 (https://api.semanticscholar.org/CorpusID:1380135).
62. Watrous, John (April 21, 2018). "Quantum Computational Complexity". arXiv:0804.3401 (https://arxiv.org/abs/0804.3401) [quant-ph (https://arxiv.org/archive/quant-ph)].
63. Tušarová, Tereza (2004). "Quantum complexity classes". arXiv:cs/0409051 (https://arxiv.org/abs/cs/0409051).
64. Lund, A. P.; Bremner, Michael J.; Ralph, T. C. (2017-04-13). "Quantum sampling problems, BosonSampling and quantum supremacy". *npj Quantum Information*. **3** (1): 15. arXiv:1702.03061 (https://arxiv.org/abs/1702.03061). Bibcode:2017npjQI...3...15L (https://ui.adsabs.harvard.edu/abs/2017npjQI...3...15L). doi:10.1038/s41534-017-0018-2 (https://doi.org/10.1038%2Fs41534-017-0018-2). ISSN 2056-6387 (https://search.worldcat.org/issn/2056-6387). S2CID 54628108 (https://api.semanticscholar.org/CorpusID:54628108).

65. Gard, Bryan T.; Motes, Keith R.; Olson, Jonathan P.; Rohde, Peter P.; Dowling, Jonathan P. (August 2015). "An introduction to boson-sampling". *From Atomic to Mesoscale: the Role of Quantum Coherence in Systems of Various Complexities*. World Scientific. pp. 167–192. arXiv:1406.6767 (https://arxiv.org/abs/1406.6767). doi:10.1142/9789814678704_0008 (https://doi.org/10.1142%2F9789814678704_0008). ISBN 978-981-4678-70-4. S2CID 55999387 (https://api.semanticscholar.org/CorpusID:55999387).
66. Bremner, Michael J.; Montanaro, Ashley; Shepherd, Dan J. (2016-08-18). "Average-case complexity versus approximate simulation of commuting quantum computations". *Physical Review Letters*. **117** (8): 080501. arXiv:1504.07999 (https://arxiv.org/abs/1504.07999). Bibcode:2016PhRvL.117h0501B (https://ui.adsabs.harvard.edu/abs/2016PhRvL.117h0501B). doi:10.1103/PhysRevLett.117.080501 (https://doi.org/10.1103%2FPhysRevLett.117.080501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 27588839 (https://pubmed.ncbi.nlm.nih.gov/27588839). S2CID 8590553 (https://api.semanticscholar.org/CorpusID:8590553).
67. Jordan, Stephen. "Quantum Algorithm Zoo" (https://web.archive.org/web/20180429014516/https://math.nist.gov/quantum/zoo/). *math.nist.gov*. Archived from the original (http://math.nist.gov/quantum/zoo/) on 2018-04-29. Retrieved 2017-07-29.
68. Shor, P. (1999-01-01). "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Review*. **41** (2): 303–332. arXiv:quant-ph/9508027 (https://arxiv.org/abs/quant-ph/9508027). Bibcode:1999SIAMR..41..303S (https://ui.adsabs.harvard.edu/abs/1999SIAMR..41..303S). doi:10.1137/S0036144598347011 (https://doi.org/10.1137%2FS0036144598347011). ISSN 0036-1445 (https://search.worldcat.org/issn/0036-1445).
69. Rubinstein, Michael (2006-10-19). "The distribution of solutions to xy = N mod a with an application to factoring integers". arXiv:math/0610612 (https://arxiv.org/abs/math/0610612).
70. Babai, László; Beals, Robert; Seress, Ákos (2009). "Polynomial-time theory of matrix groups". *Proceedings of the forty-first annual ACM symposium on Theory of computing*. STOC '09. New York, New York, United States: Association for Computing Machinery. pp. 55–64. CiteSeerX 10.1.1.674.9429 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.674.9429). doi:10.1145/1536414.1536425 (https://doi.org/10.1145%2F1536414.1536425). ISBN 9781605585062. S2CID 9052772 (https://api.semanticscholar.org/CorpusID:9052772).
71. Rivest, R. L.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-key Cryptosystems". *Commun. ACM*. **21** (2): 120–126. CiteSeerX 10.1.1.607.2677 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.607.2677). doi:10.1145/359340.359342 (https://doi.org/10.1145%2F359340.359342). ISSN 0001-0782 (https://search.worldcat.org/issn/0001-0782). S2CID 2873616 (https://api.semanticscholar.org/CorpusID:2873616).
72. Martín-López, Enrique; Laing, Anthony; Lawson, Thomas; Alvarez, Roberto; Zhou, Xiao-Qi; O'Brien, Jeremy L. (November 2012). "Experimental realization of Shor's quantum factoring algorithm using qubit recycling". *Nature Photonics*. **6** (11): 773–776. arXiv:1111.4147 (https://arxiv.org/abs/1111.4147). Bibcode:2012NaPho...6..773M (https://ui.adsabs.harvard.edu/abs/2012NaPho...6..773M). doi:10.1038/nphoton.2012.259 (https://doi.org/10.1038%2Fnphoton.2012.259). ISSN 1749-4893 (https://search.worldcat.org/issn/1749-4893). S2CID 46546101 (https://api.semanticscholar.org/CorpusID:46546101).
73. Fowler, Austin G.; Mariantoni, Matteo; Martinis, John M.; Cleland, Andrew N. (2012-09-18). "Surface codes: Towards practical large-scale quantum computation". *Physical Review A*. **86** (3): 032324. arXiv:1208.0928 (https://arxiv.org/abs/1208.0928). Bibcode:2012PhRvA..86c2324F (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86c2324F). doi:10.1103/PhysRevA.86.032324 (https://doi.org/10.1103%2FPhysRevA.86.032324). S2CID 119277773 (https://api.semanticscholar.org/CorpusID:119277773).

74. Rahimi-Keshari, Saleh; Ralph, Timothy C.; Caves, Carlton M. (2016-06-20). "Sufficient Conditions for Efficient Classical Simulation of Quantum Optics". *Physical Review X*. **6** (2): 021039. arXiv:1511.06526 (https://arxiv.org/abs/1511.06526). Bibcode:2016PhRvX...6b1039R (https://ui.adsabs.harvard.edu/abs/2016PhRvX...6b1039R). doi:10.1103/PhysRevX.6.021039 (https://doi.org/10.1103%2FPhysRevX.6.021039). S2CID 23490704 (https://api.semanticscholar.org/CorpusID:23490704).
75. Carolan, Jacques; Harrold, Christopher; Sparrow, Chris; Martín-López, Enrique; Russell, Nicholas J.; Silverstone, Joshua W.; Shadbolt, Peter J.; Matsuda, Nobuyuki; Oguma, Manabu (2015-08-14). "Universal linear optics". *Science*. **349** (6249): 711–716. arXiv:1505.01182 (https://arxiv.org/abs/1505.01182). doi:10.1126/science.aab3642 (https://doi.org/10.1126%2Fscience.aab3642). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 26160375 (https://pubmed.ncbi.nlm.nih.gov/26160375). S2CID 19067232 (https://api.semanticscholar.org/CorpusID:19067232).
76. Clifford, Peter; Clifford, Raphaël (2017-06-05). "The Classical Complexity of Boson Sampling". arXiv:1706.01260 (https://arxiv.org/abs/1706.01260) [cs.DS (https://arxiv.org/archive/cs.DS)].
77. Neville, Alex; Sparrow, Chris; Clifford, Raphaël; Johnston, Eric; Birchall, Patrick M.; Montanaro, Ashley; Laing, Anthony (2017-10-02). "No imminent quantum supremacy by boson sampling". *Nature Physics*. **13** (12): 1153–1157. arXiv:1705.00686 (https://arxiv.org/abs/1705.00686). Bibcode:2017arXiv170500686N (https://ui.adsabs.harvard.edu/abs/2017arXiv170500686N). doi:10.1038/nphys4270 (https://doi.org/10.1038%2Fnphys4270). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 73635825 (https://api.semanticscholar.org/CorpusID:73635825).
78. De Raedt, Hans; Jin, Fengping; Willsch, Dennis; Willsch, Madita; Yoshioka, Naoki; Ito, Nobuyasu; Yuan, Shengjun; Michielsen, Kristel (November 2018). "Massively parallel quantum computer simulator, eleven years later" (https://doi.org/10.1016%2Fj.cpc.2018.11.005). *Computer Physics Communications*. **237**: 47–61. arXiv:1805.04708 (https://arxiv.org/abs/1805.04708). doi:10.1016/j.cpc.2018.11.005 (https://doi.org/10.1016%2Fj.cpc.2018.11.005).
79. Pednault, Edwin; John A. Gunnels; Giacomo Nannicini; Lior Horesh; Thomas Magerlein; Edgar Solomonik; Robert Wisnieff (October 2017). "Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits". arXiv:1710.05867 (https://arxiv.org/abs/1710.05867) [quant-ph (https://arxiv.org/archive/quant-ph)].
80. "Quantum Supremacy Using a Programmable Superconducting Processor" (http://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html). *Google AI Blog*. Retrieved 2019-11-02.
81. Metz, Cade (23 October 2019). "Google Claims a Quantum Breakthrough That Could Change Computing" (https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html). *The New York Times*. Retrieved 14 January 2020.
82. Edwin Pednault; John Gunnels; Giacomo Nannicini; Lior Horesh; Robert Wisnieff (October 2019). "Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits". arXiv:1910.09534 (https://arxiv.org/abs/1910.09534) [quant-ph (https://arxiv.org/archive/quant-ph)].
83. "Google and IBM Clash Over Quantum Supremacy Claim" (https://www.quantamagazine.org/google-and-ibm-clash-over-quantum-supremacy-claim-20191023/). *Quanta Magazine*. 23 October 2019. Retrieved 2020-10-29.
84. Kalai, Gil (2011-06-02). "How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation". arXiv:1106.0485 (https://arxiv.org/abs/1106.0485) [quant-ph (https://arxiv.org/archive/quant-ph)].

85. Shor, Peter W. (1995-10-01). "Scheme for reducing decoherence in quantum computer memory". *Physical Review A*. **52** (4): R2493–R2496. Bibcode:1995PhRvA..52.2493S (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.2493S). doi:10.1103/PhysRevA.52.R2493 (https://doi.org/10.1103%2FPhysRevA.52.R2493). PMID 9912632 (https://pubmed.ncbi.nlm.nih.gov/9912632).
86. Steane, A. M. (1996-07-29). "Error Correcting Codes in Quantum Theory". *Physical Review Letters*. **77** (5): 793–797. Bibcode:1996PhRvL..77..793S (https://ui.adsabs.harvard.edu/abs/1996PhRvL..77..793S). doi:10.1103/PhysRevLett.77.793 (https://doi.org/10.1103%2FPhysRevLett.77.793). PMID 10062908 (https://pubmed.ncbi.nlm.nih.gov/10062908).
87. Aharonov, Dorit; Ben-Or, Michael (1999-06-30). "Fault-Tolerant Quantum Computation With Constant Error Rate". arXiv:quant-ph/9906129 (https://arxiv.org/abs/quant-ph/9906129).
88. Knill, E. (2005-03-03). "Quantum computing with realistically noisy devices". *Nature*. **434** (7029): 39–44. arXiv:quant-ph/0410199 (https://arxiv.org/abs/quant-ph/0410199). Bibcode:2005Natur.434...39K (https://ui.adsabs.harvard.edu/abs/2005Natur.434...39K). doi:10.1038/nature03350 (https://doi.org/10.1038%2Fnature03350). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 15744292 (https://pubmed.ncbi.nlm.nih.gov/15744292). S2CID 4420858 (https://api.semanticscholar.org/CorpusID:4420858).
89. Kalai, Gil (2016-05-03). "The Quantum Computer Puzzle (Expanded Version)". arXiv:1605.00992 (https://arxiv.org/abs/1605.00992) [quant-ph (https://arxiv.org/archive/quant-ph)].
90. Dyakonov, M. I. (2007). "Is Fault-Tolerant Quantum Computation Really Possible?". In Luryi, S.; Xu, J.; Zaslavsky, A. (eds.). *Future Trends in Microelectronics. Up the Nano Creek*. Wiley. pp. 4–18. arXiv:quant-ph/0610117 (https://arxiv.org/abs/quant-ph/0610117). Bibcode:2006quant.ph.10117D (https://ui.adsabs.harvard.edu/abs/2006quant.ph.10117D).
91. Board, The Editorial (17 December 2019). "Opinion | Achieving Quantum Wokeness" (https://www.wsj.com/articles/achieving-quantum-wokeness-11576540808). *Wall Street Journal*. Retrieved 2019-12-21.
92. Knapton, Sarah (2019-12-17). "Academics derided for claiming 'quantum supremacy' is a racist and colonialist term" (https://www.telegraph.co.uk/science/2019/12/17/academics-derided-claiming-quantum-supremacy-racist-colonialist/). *The Telegraph*. ISSN 0307-1235 (https://search.worldcat.org/issn/0307-1235). Retrieved 2019-12-21.
93. Palacios-Berraquero, Carmen; Mueck, Leonie; Persaud, Divya M. (2019-12-10). "Instead of 'supremacy' use 'quantum advantage' " (https://doi.org/10.1038%2Fd41586-019-03781-0). *Nature*. **576** (7786): 213. doi:10.1038/d41586-019-03781-0 (https://doi.org/10.1038%2Fd41586-019-03781-0). PMID 31822842 (https://pubmed.ncbi.nlm.nih.gov/31822842).
94. Ball, Philip (17 December 2020). "Physicists in China challenge Google's 'quantum advantage' " (https://www.nature.com/articles/d41586-020-03434-7). *Nature*. **588** (7838): 380. Bibcode:2020Natur.588..380B (https://ui.adsabs.harvard.edu/abs/2020Natur.588..380B). doi:10.1038/d41586-020-03434-7 (https://doi.org/10.1038%2Fd41586-020-03434-7). PMID 33273711 (https://pubmed.ncbi.nlm.nih.gov/33273711). S2CID 227282052 (https://api.semanticscholar.org/CorpusID:227282052). Retrieved 16 December 2020.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_supremacy&oldid=1243492157"

WIKIPEDIA
The Free Encyclopedia

Quantum volume

Quantum volume is a metric that measures the capabilities and error rates of a quantum computer. It expresses the maximum size of square quantum circuits that can be implemented successfully by the computer. The form of the circuits is independent from the quantum computer architecture, but compiler can transform and optimize it to take advantage of the computer's features. Thus, quantum volumes for different architectures can be compared.

The current world record for highest quantum volume as of September 2024 is 2^{100} accomplished by Dynex's n.quantum computing platform[1], outperforming the previous record from April 2024 of 2^{20} by Quantinuum's H1-1 20-qubit ion trap quantum computer.[2].

Introduction

Quantum computers are difficult to compare. Quantum volume is a single number designed to show all around performance. It is a measurement and not a calculation, and takes into account several features of a quantum computer, starting with its number of qubits—other measures used are gate and measurement errors, crosstalk and connectivity.[3][4][5]

IBM defined its Quantum Volume metric[6] because a classical computer's transistor count and a quantum computer's quantum bit count aren't the same. Qubits decohere with a resulting loss of performance so a few fault tolerant bits are more valuable as a performance measure than a larger number of noisy, error-prone qubits.[7][8]

Generally, the larger the quantum volume, the more complex the problems a quantum computer can solve.[9]

Alternative benchmarks, such as Cross-entropy benchmarking, reliable Quantum Operations per Second (rQOPS) proposed by Microsoft, Circuit Layer Operations Per Second (CLOPS) proposed by IBM and IonQ's Algorithmic Qubits, have also been proposed.[10][11]

Definition

Original Definition

The quantum volume of a quantum computer was originally defined in 2018 by Nikolaj Moll *et al.*[12] However, since around 2021 that definition has been supplanted by IBM's 2019 redefinition.[13][14] The original definition depends on the number of qubits N as well as the number of steps that can be executed, the circuit depth d

$$\tilde{V}_Q = \min[N, d(N)]^2.$$

The circuit depth depends on the effective error rate ε_{eff} as

$$d \simeq \frac{1}{N\varepsilon_{\text{eff}}}.$$

The effective error rate ε_{eff} is defined as the average error rate of a two-qubit gate. If the physical two-qubit gates do not have all-to-all connectivity, additional SWAP gates may be needed to implement an arbitrary two-qubit gate and $\varepsilon_{\text{eff}} > \varepsilon$, where ε is the error rate of the physical two-qubit gates. If more complex hardware gates are available, such as the three-qubit Toffoli gate, it is possible that $\varepsilon_{\text{eff}} < \varepsilon$.

The allowable circuit depth decreases when more qubits with the same effective error rate are added. So with these definitions, as soon as $d(N) < N$, the quantum volume goes down if more qubits are added. To run an algorithm that only requires $n < N$ qubits on an N-qubit machine, it could be beneficial to select a subset of qubits with good connectivity. For this case, Moll *et al.* [12] give a refined definition of quantum volume.

$$V_Q = \max_{n<N} \left\{ \min \left[n, \frac{1}{n\varepsilon_{\text{eff}}(n)} \right]^2 \right\},$$

where the maximum is taken over an arbitrary choice of n qubits.

IBM's redefinition

In 2019, IBM's researchers modified the quantum volume definition to be an exponential of the circuit size, stating that it corresponds to the complexity of simulating the circuit on a classical computer:[6][15]

$$\log_2 V_Q = \arg\max_{n \leq N} \{\min [n, d(n)]\}$$

Achievement history

Date	Quantum volume[a]	Qubit count	Manufacturer	System name and reference
2020, January	2^5	28	IBM	"Raleigh"[16]
2020, June	2^6	6	Honeywell	[17]
2020, August	2^6	27	IBM	Falcon r4 "Montreal"[18]
2020, November	2^7	10	Honeywell	"System Model H1"[19]
2020, December	2^7	27	IBM	Falcon r4 "Montreal"[20]
2021, March	2^9	10	Honeywell	"System Model H1"[21]
2021, July	2^{10}	10	Honeywell	"Honeywell System H1"[22]
2021, December	2^{11}	12	Quantinuum (previously Honeywell)	"Quantinuum System Model H1-2"[23]
2022, April	2^8	27	IBM	Falcon r10 "Prague"[24]
2022, April	2^{12}	12	Quantinuum	"Quantinuum System Model H1-2"[25]
2022, May	2^9	27	IBM	Falcon r10 "Prague"[26]
2022, September	2^{13}	20	Quantinuum	"Quantinuum System Model H1-1"[27]
2023, February	2^7	24	Alpine Quantum Technologies	"Compact Ion-Trap Quantum Computing Demonstrator"[28]
2023, February	2^{15}	20	Quantinuum	"Quantinuum System Model H1-1"[29]
2023, May	2^{16}	32	Quantinuum	"Quantinuum System Model H2"[30]
2023, June	2^{19}	20	Quantinuum	"Quantinuum System Model H1-1"[31]
2024, April	2^{20}	20	Quantinuum	"Quantinuum System Model H1-1"[2]
2024, September	2^{100}	100	Dynex	"Dynex n.Quantum Computing Platform"[1]

Volumetric benchmarks

The quantum volume benchmark defines a family of *square* circuits, whose number of qubits N and depth d are the same. Therefore, the output of this benchmark is a single number. However, a proposed generalization is the volumetric benchmark[32] framework, which defines a family of *rectangular* quantum circuits, for which N and d are uncoupled to allow the study of time/space performance trade-offs, thereby sacrificing the simplicity of a single-figure benchmark.

Volumetric benchmarks can be generalized not only to account for uncoupled N and d dimensions, but also to test different types of quantum circuits. While quantum volume benchmarks the quantum computer's ability to implement a specific type of *randomized circuits*, these can, in principle, be substituted by other families of random circuits, periodic circuits,[33] or algorithm-inspired circuits. Each benchmark must have a success criterion that defines whether a processor has "passed" a given test circuit.

While these data can be analyzed in many ways, a simple method of visualization is illustrating the Pareto front of the N versus d trade-off for the processor being benchmarked. This Pareto front provides information on the largest depth d a patch of a given number of qubits N can withstand, or, alternatively, the biggest patch of N qubits that can withstand executing a circuit of given depth d.

See also

- Noisy intermediate-scale quantum era
- Quantum fidelity

Notes

a. Per § IBM's redefinition

References

1. Dynex Development, Est (2024-09-11). "Dynex solidifies its leadership in quantum computing, reaching a groundbreaking milestone in Quantum Volume" (https://dynexcoin.medium.com/dynex-solidifies-its-leadership-in-quantum-computing-reaching-a-groundbreaking-milestone-in-4da9d4e0fb3a). *dynex.co*. Retrieved 2024-09-11.
2. "Quantinuum extends its significant lead in quantum computing, achieving historic milestones for hardware fidelity and Quantum Volume" (https://www.quantinuum.com/news/quantinuum-extends-its-significant-lead-in-quantum-computing-achieving-historic-milestones-for-hardware-fidelity-and-quantum-volume). *www.quantinuum.com*. Retrieved 2024-04-17.
3. "Honeywell claims to have built the highest-performing quantum computer available" (https://phys.org/news/2020-06-honeywell-built-highest-performing-quantum.html). *phys.org*. Retrieved 2020-06-22.
4. Smith-Goodson, Paul. "Quantum Volume: A Yardstick To Measure The Performance Of Quantum Computers" (https://www.forbes.com/sites/moorinsights/2019/11/23/quantum-volume-a-yardstick-to-measure-the-power-of-quantum-computers/). *Forbes*. Retrieved 2020-06-22.
5. "Measuring Quantum Volume" (https://community.qiskit.org/textbook/ch-quantum-hardware/measuring-quantum-volume.html). *Qiskit.org*. Retrieved 2020-08-21.
6. Cross, Andrew W.; Bishop, Lev S.; Sheldon, Sarah; Nation, Paul D.; Gambetta, Jay M. (2019). "Validating quantum computers using randomized model circuits" (https://journals.aps.org/pra/abstract/10.1103/PhysRevA.100.032328). *Phys. Rev. A*. **100** (3): 032328. arXiv:1811.12926 (https://arxiv.org/abs/1811.12926). Bibcode:2019PhRvA.100c2328C (https://ui.adsabs.harvard.edu/abs/2019PhRvA.100c2328C). doi:10.1103/PhysRevA.100.032328 (https://doi.org/10.1103%2FPhysRevA.100.032328). S2CID 119408990 (https://api.semanticscholar.org/CorpusID:119408990). Retrieved 2020-10-02.

7. Mandelbaum, Ryan F. (2020-08-20). "What Is Quantum Volume, Anyway?" (https://medium.com/qiskit/what-is-quantum-volume-anyway-a4dff801c36f). *Medium Qiskit*. Retrieved 2020-08-21.
8. Sanders, James (August 12, 2019). "Why quantum volume is vital for plotting the path to quantum advantage" (https://www.techrepublic.com/article/why-quantum-volume-is-vital-for-plotting-the-path-to-quantum-advantage/). *TechRepublic*. Retrieved 2020-08-22.
9. Patty, Lee (2020). "Quantum Volume: The Power of Quantum Computers" (https://www.honeywell.com/content/honeywell/us/en/newsroom/news/2020/03/quantum-volume-the-power-of-quantum-computers.html). *www.honeywell.com*. Chief Scientist for Honeywell Quantum Solutions. Retrieved 2020-08-21.
10. Yirka, Bob (2023-06-24). "Microsoft claims to have achieved first milestone in creating a reliable and practical quantum computer" (https://phys.org/news/2023-06-microsoft-milestone-reliable-quantum.html). *phys.org*. Retrieved 2024-07-01.
11. Leprince-Ringuet, Daphne (2021-11-02). "Quantum computing: IBM just created this new way to measure the speed of quantum processors" (https://www.zdnet.com/article/quantum-computing-this-is-how-ibm-is-now-measuring-the-speed-of-its-quantum-processors/). *ZDNet*. Retrieved 2024-07-01.
12. Moll, Nikolaj; Barkoutsos, Panagiotis; Bishop, Lev S; Chow, Jerry M; Cross, Andrew; Egger, Daniel J; Filipp, Stefan; Fuhrer, Andreas; Gambetta, Jay M; Ganzhorn, Marc; Kandala, Abhinav; Mezzacapo, Antonio; Müller, Peter; Riesswe introd, Walter; Salis, Gian; Smolin, John; Tavernelli, Ivano; Temme, Kristan (2018). "Quantum optimization using variational algorithms on near-term quantum devices" (https://doi.org/10.1088%2F2058-9565%2Faab822). *Quantum Science and Technology*. **3** (3): 030503. arXiv:1710.01022 (https://arxiv.org/abs/1710.01022). Bibcode:2018QS&T....3c0503M (https://ui.adsabs.harvard.edu/abs/2018QS&T....3c0503M). doi:10.1088/2058-9565/aab822 (https://doi.org/10.1088%2F2058-9565%2Faab822).
13. Baldwin, Charles; Mayer, Karl (2022). "Re-examining the quantum volume test: Ideal distributions, compiler optimizations, confidence intervals, and scalable resource estimations". *Quantum*. **6**: 707. arXiv:2110.14808 (https://arxiv.org/abs/2110.14808). Bibcode:2022Quant...6..707B (https://ui.adsabs.harvard.edu/abs/2022Quant...6..707B). doi:10.22331/q-2022-05-09-707 (https://doi.org/10.22331%2Fq-2022-05-09-707). S2CID 240070758 (https://api.semanticscholar.org/CorpusID:240070758).
14. Miller, Keith (2022-07-14). "An Improved Volumetric Metric for Quantum Computers via more Representative Quantum Circuit Shapes". arXiv:2207.02315 (https://arxiv.org/abs/2207.02315) [quant-ph (https://arxiv.org/archive/quant-ph)].
15. https://pennylane.ai/qml/demos/quantum_volume.html (archived (https://web.archive.org/web/20201216123226/https://pennylane.ai/qml/demos/quantum_volume.html))
16. "IBM Doubles Its Quantum Computing Power Again" (https://www.forbes.com/sites/moorinsights/2020/01/08/ibm-doubles-its-quantum-computing-power-again/). *Forbes*. 2020-01-08.
17. Samuel K. Moore (2020-06-24). "Honeywell Claims It Has Most Powerful Quantum Computer" (https://spectrum.ieee.org/honeywell-claims-it-has-most-powerful-quantum-computer). *IEEE Spectrum*.
18. Condon, Stephanie (August 20, 2020). "IBM hits new quantum computing milestone" (https://www.zdnet.com/article/ibm-hits-new-quantum-computing-milestone/). *ZDNet*. Retrieved 2020-08-21.
19. Samuel K. Moore (2020-11-10). "Rapid Scale-Up of Commercial Ion-Trap Quantum Computers" (https://spectrum.ieee.org/commercial-iontrap-quantum-computers-showing-rapid-scaleup). *IEEE Spectrum*.

20. Gambetta, Jay [@jaygambetta] (2020-12-03). "On the same system (IBM Q System One - Montreal) that we hit a quantum volume of 64 the team recently achieved a quantum volume of 128. This year's progress in the quality of quantum circuits has been amazing. https://t.co/pBYmLkmSoS" (https://x.com/jaygambetta/status/1334526177642491904) (Tweet). Archived (https://web.archive.org/web/20221021003459/http://twitter.com/jaygambetta/status/1334526177642491904) from the original on 2022-10-21. Retrieved 2022-12-04 – via Twitter.
21. Leprince-Ringuet, Daphne. "Quantum computing: Honeywell just quadrupled the power of its computer" (https://www.zdnet.com/article/quantum-computing-honeywell-just-quadrupled-the-power-of-its-computer/). *ZDNet*. Retrieved 2021-03-11.
22. "Honeywell and Cambridge Quantum Reach New Milestones" (https://www.honeywell.com/us/en/press/2021/07/honeywell-and-cambridge-quantum-reach-new-milestones). *www.honeywell.com*. Retrieved 2021-07-23.
23. "Demonstrating Benefits of Quantum Upgradable Design Strategy: System Model H1-2 First to Prove 2,048 Quantum Volume" (https://www.quantinuum.com/pressrelease/demonstrating-benefits-of-quantum-upgradable-design-strategy-system-model-h1-2-first-to-prove-2-048-quantum-volume). *www.quantinuum.com*. Retrieved 2022-01-04.
24. "Pushing quantum performance forward with our highest quantum volume yet" (https://research.ibm.com/blog/quantum-volume-256). *IBM Research Blog*. 6 April 2022.
25. "Quantinuum Announces Quantum Volume 4096 Achievement" (https://www.quantinuum.com/pressrelease/quantinuum-announces-quantum-volume-4096-achievement). *www.quantinuum.com*. Retrieved 2022-04-14.
26. Gambetta, Jay [@jaygambetta] (2022-05-25). "Just a little update from the IBM Quantum team. QV of 512 achieved😀. Our new gate architecture (Falcon R10) continues to allow higher fidelity and low crosstalk and as a result better quality circuits. Two jumps in QV in the last 2 months. https://t.co/szAKCAD4gA" (https://x.com/jaygambetta/status/1529489786242744320) (Tweet). Archived (https://web.archive.org/web/20220528065407/https://twitter.com/jaygambetta/status/1529489786242744320) from the original on 2022-05-28. Retrieved 2022-12-04 – via Twitter.
27. Smith-Goodson, Paul (2022-10-06). "Quantinuum Is On A Roll – 17 Significant Quantum Computing Achievements In 12 Months" (https://web.archive.org/web/20221006170105/https://www.forbes.com/sites/moorinsights/2022/10/06/quantinuum-is-on-a-roll--17-significant-quantum-computing-achievements-in-12-months/). *Forbes*. Archived from the original on 2022-10-06. Retrieved 2023-02-24.
28. Monz, Thomas (2023-02-10). "State of Quantum Computing in Europe: AQT pushing performance with a Quantum Volume of 128" (https://www.aqt.eu/aqt-pushing-performance-with-a-quantum-volume-of-128/). *techmonitor.ai*. Retrieved 2023-05-09.
29. Morrison, Ryan (2023-02-23). "Quantinuum hits quantum performance milestone" (https://techmonitor.ai/hardware/quantinuum-hits-quantum-performance-milestone). *techmonitor.ai*. Retrieved 2023-02-24.
30. Moses, S.A. (2023-05-09). "A Race-Track Trapped-Ion Quantum Processor". *Physical Review X*. **13** (4): 041052. arXiv:2305.03828 (https://arxiv.org/abs/2305.03828). Bibcode:2023PhRvX..13d1052M (https://ui.adsabs.harvard.edu/abs/2023PhRvX..13d1052M). doi:10.1103/PhysRevX.13.041052 (https://doi.org/10.1103%2FPhysRevX.13.041052).
31. Morrison, Ryan (2023-06-30). "Quantinuum H-Series quantum computer accelerates through 3 more performance records for quantum volume" (https://www.quantinuum.com/news/quantinuum-h-series-quantum-computer-accelerates-through-3-more-performance-records-for-quantum-volume-217-218-and-219). *quantinuum*. Retrieved 2023-06-30.

32. Blume-Kohout, Robin; Young, Kevin C. (2020-11-15). "A volumetric framework for quantum computer benchmarks". *Quantum*. **4**: 362. arXiv:1904.05546 (https://arxiv.org/abs/1904.05546). Bibcode:2020Quant...4..362B (https://ui.adsabs.harvard.edu/abs/2020Quant...4..362B). doi:10.22331/q-2020-11-15-362 (https://doi.org/10.22331%2Fq-2020-11-15-362). ISSN 2521-327X (https://search.worldcat.org/issn/2521-327X).
33. Proctor, Timothy; Rudinger, Kenneth; Young, Kevin; Nielsen, Erik; Blume-Kohout, Robin (2021-12-20). "Measuring the capabilities of quantum computers". *Nature Physics*. **18** (1). Springer Science and Business Media LLC: 75–79. arXiv:2008.11294 (https://arxiv.org/abs/2008.11294). doi:10.1038/s41567-021-01409-7 (https://doi.org/10.1038%2Fs41567-021-01409-7). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_volume&oldid=1245582876"

WIKIPEDIA
The Free Encyclopedia

Randomized benchmarking

Randomized benchmarking is an experimental method for measuring the average error rates of quantum computing hardware platforms. The protocol estimates the average error rates by implementing long sequences of randomly sampled quantum gate operations.[1] Randomized benchmarking is the industry-standard protocol used by quantum hardware developers such as IBM[2] and Google [3] to test the performance of the quantum operations.

The original theory of randomized benchmarking, proposed by Joseph Emerson and collaborators,[1] considered the implementation of sequences of Haar-random operations, but this had several practical limitations. The now-standard protocol for randomized benchmarking (RB) relies on uniformly random Clifford operations, as proposed in 2006 by Dankert *et al.* [4] as an application of the theory of unitary t-designs. In current usage randomized benchmarking sometimes refers to the broader family of generalizations of the 2005 protocol involving different random gate sets [5][6][7][8][9][10][11][12][13][14] that can identify various features of the strength and type of errors affecting the elementary quantum gate operations. Randomized benchmarking protocols are an important means of verifying and validating quantum operations and are also routinely used for the optimization of quantum control procedures. [15]

Overview

Randomized benchmarking offers several key advantages over alternative approaches to error characterization. For example, the number of experimental procedures required for full characterization of errors (called tomography) grows exponentially with the number of quantum bits (called qubits). This makes tomographic methods impractical for even small systems of just 3 or 4 qubits. In contrast, randomized benchmarking protocols are the only known approaches to error characterization that scale efficiently as number of qubits in the system increases.[4] Thus RB can be applied in practice to characterize errors in arbitrarily large quantum processors. Additionally, in experimental quantum computing, procedures for state preparation and measurement (SPAM) are also error-prone, and thus quantum process tomography is unable to distinguish errors associated with gate operations from errors associated with SPAM. In contrast, RB protocols are robust to state-preparation and measurement errors [1][7]

Randomized benchmarking protocols estimate key features of the errors that affect a set of quantum operations by examining how the observed fidelity of the final quantum state decreases as the length of the random sequence increases. If the set of operations satisfies certain mathematical properties,[1][4][7][16][10][11][12] such as comprising a sequence of twirls [5][17] with unitary two-designs,[4] then the measured decay can be shown to be an invariant exponential with a rate fixed uniquely by features of the error model.

History

Randomized benchmarking was proposed in *Scalable noise estimation with random unitary operators*,[1] where it was shown that long sequences of quantum gates sampled *uniformly* at random from the Haar measure on the group SU(*d*) would lead to an exponential decay at a rate that was uniquely fixed by the error model. Emerson, Alicki and Zyczkowski also showed, under the assumption of gate-independent errors, that the measured decay rate is directly related to an important figure of merit, the average gate fidelity and independent of the choice of initial state and any errors in the initial state, as well as the specific random sequences of quantum gates. This protocol applied for arbitrary dimension d and an arbitrary number n of qubits, where $d=2^n$. The SU(d) RB protocol had two important limitations that were overcome in a modified protocol proposed by Dankert *et al.*,[4] who proposed sampling the gate operations uniformly at random from any unitary two-design, such as the Clifford group. They proved that this would produce the same exponential decay rate as the random SU(d) version of the protocol proposed in Emerson *et al.*.[1] This follows from the observation that a random sequence of gates is equivalent to an independent sequence of twirls under that group, as conjectured in [1] and later proven in.[5] This Clifford-group approach to Randomized Benchmarking [1][4] is the now standard method for assessing error rates in quantum computers. A variation of this protocol was proposed by NIST in 2008 [6] for the first experimental implementation of an RB-type for single qubit gates. However, the sampling of random gates in the NIST protocol was later proven not to reproduce any unitary two-design.[12] The NIST RB protocol was later shown to also produce an exponential fidelity decay, albeit with a rate that depends on non-invariant features of the error model [12]

In recent years a rigorous theoretical framework has been developed for Clifford-group RB protocols to show that they work reliably under very broad experimental conditions. In 2011 and 2012, Magesan *et al.*[7][8] proved that the exponential decay rate is fully robust to arbitrary state preparation and measurement errors (SPAM). They also proved a connection between the average gate fidelity and diamond norm metric of error that is relevant to the fault-tolerant threshold. They also provided evidence that the observed decay was exponential and related to the average gate fidelity even if the error model varied across the gate operations, so-called gate-dependent errors, which is the experimentally realistic situation. In 2018, Wallman [16] and Dugas *et al.*,[11] showed that, despite concerns raised in,[18] even under very strong gate-dependence errors the standard RB protocols produces an exponential decay at a rate that precisely measures the average gate-fidelity of the experimentally relevant errors. The results of Wallman.[16] in particular proved that the RB error rate is so robust to gate-dependent errors models that it provides an extremely sensitive tool for detecting non-Markovian errors. This follows because under a standard RB experiment only non-Markovian errors (including time-dependent Markovian errors) can produce a statistically significant deviation from an exponential decay [16]

The standard RB protocol was first implemented for single qubit gate operations in 2012 at Yale on a superconducting qubit.[19] A variation of this standard protocol that is only defined for single qubit operations was implemented by NIST in 2008 [6] on a trapped ion. The first implementation of the standard RB protocol for two-qubit gates was performed in 2012 at NIST for a system of two trapped ions [20]

References

1. Emerson, Joseph; Alicki, Robert; Zyczkowski, Karol (2005). "Scalable noise estimation with random unitary operators". *Journal of Optics B: Quantum and Semiclassical Optics*. **7** (10): S347. arXiv:quant-ph/0503243 (https://arxiv.org/abs/quant-ph/0503243).

Bibcode:2005JOptB...7S.347E (https://ui.adsabs.harvard.edu/abs/2005JOptB...7S.347E). doi:10.1088/1464-4266/7/10/021 (https://doi.org/10.1088%2F1464-4266%2F7%2F10%2F021). S2CID 17729419 (https://api.semanticscholar.org/CorpusID:17729419).

2. "Randomized Benchmarking — Qiskit textbook" (https://qiskit.org/textbook/ch-quantum-hardware/randomized-benchmarking.html).
3. "Cirq Qubit Characterization Example" (https://github.com/quantumlib/Cirq/blob/master/examples/qubit_characterizations_example.py). *GitHub*. 20 January 2023.
4. Dankert, Christoph; Cleve, Richard; Emerson, Joseph; Livine, Etera (2009). "Exact and Approximate Unitary 2-Designs: Constructions and Applications". *Physical Review A*. **80**: 012304. arXiv:quant-ph/0606161 (https://arxiv.org/abs/quant-ph/0606161). doi:10.1103/PhysRevA.80.012304 (https://doi.org/10.1103%2FPhysRevA.80.012304). S2CID 46914367 (https://api.semanticscholar.org/CorpusID:46914367).
5. Levi, Benjamin; Lopez, Cecilia; Emerson, Joseph; Cory, David (2007). "Efficient error characterization in quantum information processing". *Physical Review A*. **75** (2): 022314. arXiv:quant-ph/0608246 (https://arxiv.org/abs/quant-ph/0608246). Bibcode:2007PhRvA..75b2314L (https://ui.adsabs.harvard.edu/abs/2007PhRvA..75b2314L). doi:10.1103/PhysRevA.75.022314 (https://doi.org/10.1103%2FPhysRevA.75.022314). S2CID 119511781 (https://api.semanticscholar.org/CorpusID:119511781).
6. Knill, E; Leibfried, D; Reichle, R; Britton, J; Blakestad, R; Jost, J; Langer, C; Ozeri, R; Seidelin, S; Wineland, D.J. (2008). "Randomized benchmarking of quantum gates". *Physical Review A*. **77** (1): 012307. arXiv:0707.0963 (https://arxiv.org/abs/0707.0963). Bibcode:2008PhRvA..77a2307K (https://ui.adsabs.harvard.edu/abs/2008PhRvA..77a2307K). doi:10.1103/PhysRevA.77.012307 (https://doi.org/10.1103%2FPhysRevA.77.012307). S2CID 4653296 (https://api.semanticscholar.org/CorpusID:4653296).
7. Magesan, Easwar; Gambetta, Jay M.; Emerson, Joseph (2011). "Scalable and Robust Randomized Benchmarking of Quantum Processes". *Physical Review Letters*. **106** (31–9007): 180504. arXiv:1009.3639 (https://arxiv.org/abs/1009.3639). Bibcode:2011PhRvL.106r0504M (https://ui.adsabs.harvard.edu/abs/2011PhRvL.106r0504M). doi:10.1103/PhysRevLett.106.180504 (https://doi.org/10.1103%2FPhysRevLett.106.180504). PMID 21635076 (https://pubmed.ncbi.nlm.nih.gov/21635076). S2CID 40488758 (https://api.semanticscholar.org/CorpusID:40488758).
8. Magesan, Easwar; Gambetta, Jay M.; Emerson, Joseph (2012). "Characterizing quantum gates via randomized benchmarking". *Physical Review A*. **85** (1050–2947): 042311. arXiv:1109.6887 (https://arxiv.org/abs/1109.6887). Bibcode:2012PhRvA..85d2311M (https://ui.adsabs.harvard.edu/abs/2012PhRvA..85d2311M). doi:10.1103/PhysRevA.85.042311 (https://doi.org/10.1103%2FPhysRevA.85.042311). S2CID 4676920 (https://api.semanticscholar.org/CorpusID:4676920).
9. Wallman, Joel; Barnhill, Marie; Emerson, Joseph (2016). "Robust characterization of leakage errors" (https://doi.org/10.1088%2F1367-2630%2F18%2F4%2F043021). *New Journal of Physics*. **18** (4): 043021. arXiv:1412.4126 (https://arxiv.org/abs/1412.4126). Bibcode:2016NJPh...18d3021W (https://ui.adsabs.harvard.edu/abs/2016NJPh...18d3021W). doi:10.1088/1367-2630/18/4/043021 (https://doi.org/10.1088%2F1367-2630%2F18%2F4%2F043021).
10. Dugas, A; Wallman, J; Emerson, J (2015). "Characterizing universal gate sets via dihedral benchmarking". *Physical Review A*. **92** (6): 060302. arXiv:1508.06312 (https://arxiv.org/abs/1508.06312). Bibcode:2015PhRvA..92f0302C (https://ui.adsabs.harvard.edu/abs/2015PhRvA..92f0302C). doi:10.1103/PhysRevA.92.060302 (https://doi.org/10.1103%2FPhysRevA.92.060302). S2CID 67832001 (https://api.semanticscholar.org/CorpusID:67832001).

11. Dugas, Arnaud; Boone, Kristine; Wallman, Joel; Emerson, Joseph (2018). "From randomized benchmarking experiments to gate-set circuit fidelity: how to interpret randomized benchmarking decay parameters". *New Journal of Physics*. **20** (9): 092001. arXiv:1804.01122 (https://arxiv.org/abs/1804.01122). Bibcode:2018NJPh...20i2001C (https://ui.adsabs.harvard.edu/abs/2018NJPh...20i2001C). doi:10.1088/1367-2630/aadcc7 (https://doi.org/10.1088%2F1367-2630%2Faadcc7). S2CID 88509448 (https://api.semanticscholar.org/CorpusID:88509448).
12. Boone, Kristine; Dugas, Arnaud; Wallman, Joel; Emerson, Joseph (2019). "Randomized benchmarking under different gate sets". *Physical Review A*. **99** (3): 032329. arXiv:1811.01920 (https://arxiv.org/abs/1811.01920). Bibcode:2019PhRvA..99c2329B (https://ui.adsabs.harvard.edu/abs/2019PhRvA..99c2329B). doi:10.1103/PhysRevA.99.032329 (https://doi.org/10.1103%2FPhysRevA.99.032329). S2CID 53578478 (https://api.semanticscholar.org/CorpusID:53578478).
13. Wallman, Joel; Granade, Chris; Harper, Robin; Flammia, Steven (2015). "Estimating the coherence of noise" (http://stacks.iop.org/1367-2630/17/i=11/a=113020). *New Journal of Physics*. **17** (11): 113020. arXiv:1503.07865 (https://arxiv.org/abs/1503.07865). Bibcode:2015NJPh...17k3020W (https://ui.adsabs.harvard.edu/abs/2015NJPh...17k3020W). doi:10.1088/1367-2630/17/11/113020 (https://doi.org/10.1088%2F1367-2630%2F17%2F11%2F113020). S2CID 119215285 (https://api.semanticscholar.org/CorpusID:119215285).
14. Gambetta, Jay M.; Corcoles, A.D.; Merkel, Seth T.; Johnson, Blake R.; Smolin, John A.; Chow, Jerry M.; Ryan, Colm A.; Rigetti, Chad; Poletto, Stefano; Ohki, Thomas A.; Ketchen, Mark B.; Steffen, Matthias (2012). "Characterization of Addressability by Simultaneous Randomized Benchmarking". *Physical Review Letters*. **109** (31–9007): 240504. arXiv:1204.6308 (https://arxiv.org/abs/1204.6308). Bibcode:2012PhRvL.109x0504G (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109x0504G). doi:10.1103/PhysRevLett.109.240504 (https://doi.org/10.1103%2FPhysRevLett.109.240504). PMID 23368295 (https://pubmed.ncbi.nlm.nih.gov/23368295). S2CID 46340425 (https://api.semanticscholar.org/CorpusID:46340425).
15. Kelly, Julian; Barends, R; Campbell, B; Chen, Y; Chen, Z; Chiaro, B; Dunsworth, A; Fowler, Austin G; Hoi, I-C; Jeffrey, E (2014). "Optimal quantum control using randomized benchmarking". *Physical Review Letters*. **112** (24): 240504. arXiv:1403.0035 (https://arxiv.org/abs/1403.0035). Bibcode:2014PhRvL.112x0504K (https://ui.adsabs.harvard.edu/abs/2014PhRvL.112x0504K). doi:10.1103/PhysRevLett.112.240504 (https://doi.org/10.1103%2FPhysRevLett.112.240504). PMID 24996075 (https://pubmed.ncbi.nlm.nih.gov/24996075). S2CID 26689539 (https://api.semanticscholar.org/CorpusID:26689539).
16. Wallman, Joel (2018). "Randomized benchmarking with gate-dependent noise" (https://quantum-journal.org/papers/q-2018-01-29-47/pdf/?). *Quantum*. **2**: 47. arXiv:1703.09835 (https://arxiv.org/abs/1703.09835). Bibcode:2018Quant...2...47W (https://ui.adsabs.harvard.edu/abs/2018Quant...2...47W). doi:10.22331/q-2018-01-29-47 (https://doi.org/10.22331%2Fq-2018-01-29-47).
17. Emerson, Joseph; Silva, Marcus; Moussa, Osama; Ryan, Colm A.; Laforest, Martin; Baugh, Jonathan; Cory, David; Laflamme, Raymond (2007). "Symmetrized characterization of noisy quantum processes". *Science*. **317** (1095–9203): 1893–6. arXiv:0707.0685 (https://arxiv.org/abs/0707.0685). Bibcode:2007Sci...317.1893E (https://ui.adsabs.harvard.edu/abs/2007Sci...317.1893E). doi:10.1126/science.1145699 (https://doi.org/10.1126%2Fscience.1145699). PMID 17901327 (https://pubmed.ncbi.nlm.nih.gov/17901327). S2CID 14645655 (https://api.semanticscholar.org/CorpusID:14645655).
18. Proctor, T.; Rudinger, K.; Young, K.; Sarovar, M.; Blume-Kohout, R. (2017). "What Randomized Benchmarking Actually Measures". *Physical Review Letters*. **119** (13): 130502. arXiv:1702.01853 (https://arxiv.org/abs/1702.01853). Bibcode:2017PhRvL.119m0502P (https://ui.adsabs.harvard.edu/abs/2017PhRvL.119m0502P). doi:10.1103/PhysRevLett.119.130502 (https://doi.org/10.1103%2FPhysRevLett.119.130502). PMID 29341688 (https://pubmed.ncbi.nlm.nih.gov/29341688). S2CID 32869480 (https://api.semanticscholar.org/CorpusID:32869480).

19. Gambetta, Jay M; Corcoles, AD; Merkel, Seth T; Johnson, Blake R; Smolin, John A; Chow, Jerry M; Ryan, Colm; Rigetti, Chad; Poletto, S; Ohki, Thomas A (2012). "Characterization of addressability by simultaneous randomized benchmarking". *Physical Review Letters*. **109** (24): 240504. arXiv:1204.6308 (https://arxiv.org/abs/1204.6308). Bibcode:2012PhRvL.109x0504G (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109x0504G). doi:10.1103/PhysRevLett.109.240504 (https://doi.org/10.1103%2FPhysRevLett.109.240504). PMID 23368295 (https://pubmed.ncbi.nlm.nih.gov/23368295). S2CID 46340425 (https://api.semanticscholar.org/CorpusID:46340425).
20. Gaebler, John P; Meier, Adam M; Tan, Ting Rei; Bowler, Ryan; Lin, Yiheng; Hanneke, David; Jost, John D; Home, JP; Knill, Emanuel; Leibfried, Dietrich (2012). "Randomized benchmarking of multiqubit gates" (https://doi.org/10.1103%2FPhysRevLett.108.260503). *Physical Review Letters*. **108** (26): 260503. arXiv:1203.3733 (https://arxiv.org/abs/1203.3733). Bibcode:2012PhRvL.108z0503G (https://ui.adsabs.harvard.edu/abs/2012PhRvL.108z0503G). doi:10.1103/PhysRevLett.108.260503 (https://doi.org/10.1103%2FPhysRevLett.108.260503). PMID 23004946 (https://pubmed.ncbi.nlm.nih.gov/23004946).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Randomized_benchmarking&oldid=1242342141"

WIKIPEDIA
The Free Encyclopedia

Cross-entropy benchmarking

Cross-entropy benchmarking (also referred to as **XEB**) is a quantum benchmarking protocol which can be used to demonstrate quantum supremacy.[1] In XEB, a random quantum circuit is executed on a quantum computer multiple times in order to collect a set of k samples in the form of bitstrings $\{x_1, \ldots, x_k\}$. The bitstrings are then used to calculate the cross-entropy benchmark fidelity (F_{XEB}) via a classical computer, given by

$$F_{\text{XEB}} = 2^n \langle P(x_i) \rangle_k - 1 = \frac{2^n}{k} \left(\sum_{i=1}^{k} |\langle 0^n | C | x_i \rangle|^2 \right) - 1,$$

where n is the number of qubits in the circuit and $P(x_i)$ is the probability of a bitstring x_i for an ideal quantum circuit C. If $F_{XEB} = 1$, the samples were collected from a noiseless quantum computer. If $F_{\text{XEB}} = 0$, then the samples could have been obtained via random guessing.[2] This means that if a quantum computer did generate those samples, then the quantum computer is too noisy and thus has no chance of performing beyond-classical computations. Since it takes an exponential amount of resources to classically simulate a quantum circuit, there comes a point when the biggest supercomputer that runs the best classical algorithm for simulating quantum circuits can't compute the XEB. Crossing this point is known as achieving quantum supremacy; and after entering the quantum supremacy regime, XEB can only be estimated.[3]

The Sycamore processor was the first to demonstrate quantum supremacy via XEB. Instances of random circuits with $n = 53$ and 20 cycles were run to obtain an XEB of 0.0024.[3] Generating samples took 200 seconds on the quantum processor when it would have taken 10,000 years on Summit at the time of the experiment. Improvements in classical algorithms have shortened the runtime to about a week on Sunway TaihuLight thus collapsing Sycamore's claim to quantum supremacy.[4] As of 2021, the latest demonstration of quantum supremacy by Zuchongzhi 2.1 with $n = 60$, 24 cycles and an XEB of 0.000366 holds. It takes around 4 hours to generate samples on Zuchonzhi 2.1 when it would take 10,000 years on Sunway.[4]

See also

- Boson sampling

References

1. Boixo, S.; et al. (2018). "Characterizing Quantum Supremacy in Near-Term Devices". *Nature Physics*. **14** (6): 595–600. arXiv:1608.00263 (https://arxiv.org/abs/1608.00263). Bibcode:2018NatPh..14..595B (https://ui.adsabs.harvard.edu/abs/2018NatPh..14..595B). doi:10.1038/s41567-018-0124-x (https://doi.org/10.1038%2Fs41567-018-0124-x). S2CID 4167494 (https://api.semanticscholar.org/CorpusID:4167494).
2. Aaronson, S. (2021). "Open Problems Related to Quantum Query Complexity". arXiv:2109.06917 (https://arxiv.org/abs/2109.06917) [quant-ph (https://arxiv.org/archive/qua

nt-ph)].
3. Arute, F.; et al. (2019). "Quantum supremacy using a programmable superconducting processor". *Nature*. **574** (7779): 505–510. arXiv:1910.11333 (https://arxiv.org/abs/1910.11333). Bibcode:2019Natur.574..505A (https://ui.adsabs.harvard.edu/abs/2019Natur.574..505A). doi:10.1038/s41586-019-1666-5 (https://doi.org/10.1038%2Fs41586-019-1666-5). PMID 31645734 (https://pubmed.ncbi.nlm.nih.gov/31645734). S2CID 204836822 (https://api.semanticscholar.org/CorpusID:204836822).
4. Liu, X.; et al. (2021). "Redefining the Quantum Supremacy Baseline With a New Generation Sunway Supercomputer". arXiv:2111.01066 (https://arxiv.org/abs/2111.01066) [quant-ph (https://arxiv.org/archive/quant-ph)].

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cross-entropy_benchmarking&oldid=1195889836"

WIKIPEDIA
The Free Encyclopedia

Relaxation (NMR)

In magnetic resonance imaging (MRI) and nuclear magnetic resonance spectroscopy (NMR), an observable nuclear spin polarization (magnetization) is created by a homogeneous magnetic field. This field makes the magnetic dipole moments of the sample precess at the resonance (Larmor) frequency of the nuclei. At thermal equilibrium, nuclear spins precess randomly about the direction of the applied field. They become abruptly phase coherent when they are hit by radiofrequency (RF) pulses at the resonant frequency, created orthogonal to the field. The RF pulses cause the population of spin-states to be perturbed from their thermal equilibrium value. The generated transverse magnetization can then induce a signal in an RF coil that can be detected and amplified by an RF receiver. The return of the longitudinal component of the magnetization to its equilibrium value is termed *spin-lattice* **relaxation** while the loss of phase-coherence of the spins is termed *spin-spin* relaxation, which is manifest as an observed free induction decay (FID).[1]

For spin-$\frac{1}{2}$ nuclei (such as ^{1}H), the polarization due to spins oriented with the field N_- relative to the spins oriented against the field N_+ is given by the Boltzmann distribution:

$$\frac{N_+}{N_-} = e^{-\frac{\Delta E}{kT}}$$

where ΔE is the energy level difference between the two populations of spins, k is the Boltzmann constant, and T is the sample temperature. At room temperature, the number of spins in the lower energy level, N−, slightly outnumbers the number in the upper level, N+. The energy gap between the spin-up and spin-down states in NMR is minute by atomic emission standards at magnetic fields conventionally used in MRI and NMR spectroscopy. Energy emission in NMR must be induced through a direct interaction of a nucleus with its external environment rather than by spontaneous emission. This interaction may be through the electrical or magnetic fields generated by other nuclei, electrons, or molecules. Spontaneous emission of energy is a radiative process involving the release of a photon and typified by phenomena such as fluorescence and phosphorescence. As stated by Abragam, the probability per unit time of the nuclear spin-1/2 transition from the + into the - state through spontaneous emission of a photon is a negligible phenomenon.[2][3] Rather, the return to equilibrium is a much slower thermal process induced by the fluctuating local magnetic fields due to molecular or electron (free radical) rotational motions that return the excess energy in the form of heat to the surroundings.

T_1 and T_2

The decay of RF-induced NMR spin polarization is characterized in terms of two separate processes, each with their own time constants. One process, called T_1, is responsible for the loss of resonance intensity following pulse excitation. The other process, called T_2, characterizes the width or broadness of resonances. Stated more formally, T_1 is the time constant for the physical processes responsible for the relaxation of the components of the nuclear spin magnetization vector **M** parallel to the external magnetic field, $\mathbf{B}_0$ (which is conventionally designated as the z-axis). T_2 relaxation affects the coherent components

of **M** perpendicular to $\mathbf{B}_0$. In conventional NMR spectroscopy, T_1 limits the pulse repetition rate and affects the overall time an NMR spectrum can be acquired. Values of T_1 range from milliseconds to several seconds, depending on the size of the molecule, the viscosity of the solution, the temperature of the sample, and the possible presence of paramagnetic species (e.g., O_2 or metal ions).

T_1

The longitudinal (or spin-lattice) relaxation time T_1 is the decay constant for the recovery of the z component of the nuclear spin magnetization, M_z, towards its thermal equilibrium value, $M_{z,\mathrm{eq}}$. In general,

$$M_z(t) = M_{z,\mathrm{eq}} - [M_{z,\mathrm{eq}} - M_z(0)]e^{-t/T_1}$$

In specific cases:

- If **M** has been tilted into the *xy* plane, then $M_z(0) = 0$ and the recovery is simply

$$M_z(t) = M_{z,\mathrm{eq}} \left(1 - e^{-t/T_1}\right)$$

i.e. the magnetization recovers to 63% of its equilibrium value after one time constant T_1.

- In the inversion recovery experiment, commonly used to measure T_1 values, the initial magnetization is inverted, $M_z(0) = -M_{z,\mathrm{eq}}$, and so the recovery follows

$$M_z(t) = M_{z,\mathrm{eq}} \left(1 - 2e^{-t/T_1}\right)$$

T_1 relaxation involves redistributing the populations of the nuclear spin states in order to reach the thermal equilibrium distribution. By definition, this is not energy conserving. Moreover, spontaneous emission is negligibly slow at NMR frequencies. Hence truly isolated nuclear spins would show negligible rates of T_1 relaxation. However, a variety of *relaxation mechanisms* allow nuclear spins to exchange energy with their surroundings, the *lattice*, allowing the spin populations to equilibrate. The fact that T_1 relaxation involves an interaction with the surroundings is the origin of the alternative description, *spin-lattice relaxation*.

Note that the rates of T_1 relaxation (i.e., $1/T_1$) are generally strongly dependent on the NMR frequency and so vary considerably with magnetic field strength B. Small amounts of paramagnetic substances in a sample speed up relaxation very much. By degassing, and thereby removing dissolved oxygen, the T_1/T_2 of liquid samples easily go up to an order of ten seconds.

Spin saturation transfer

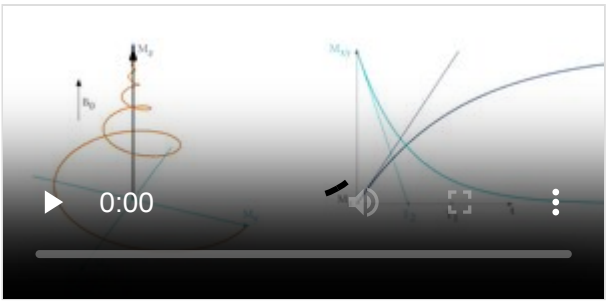
Especially for molecules exhibiting slowly relaxing (T_1) signals, the technique spin saturation transfer (SST) provides information on chemical exchange reactions. The method is widely applicable to fluxional molecules. This magnetization transfer technique provides rates, provided that they exceed $1/T_1$.[4]

T_2

The transverse (or spin-spin) relaxation time T_2 is the decay constant for the component of **M** perpendicular to $\mathbf{B}_0$, designated $\mathbf{M}_{xy}$, $\mathbf{M}_T$, or $M_\perp$. For instance, initial *xy* magnetization at time zero will decay to zero (i.e. equilibrium) as follows:

$$M_{xy}(t) = M_{xy}(0)e^{-t/T_2}$$

i.e. the transverse magnetization vector drops to 37% of its original magnitude after one time constant T_2.

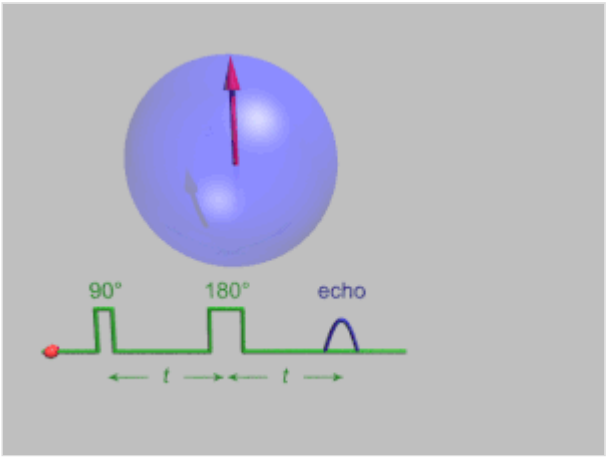


Visual representation of the spin of a proton under a constant magnetic field B_0. Visualization of the T_1 and T_2 relaxation times.

T_2 relaxation is a complex phenomenon, but at its most fundamental level, it corresponds to a decoherence of the transverse nuclear spin magnetization. Random fluctuations of the local magnetic field lead to random variations in the instantaneous NMR precession frequency of different spins. As a result, the initial phase coherence of the nuclear spins is lost, until eventually the phases are disordered and there is no net *xy* magnetization. Because T_2 relaxation involves only the phases of other nuclear spins it is often called "spin-spin" relaxation.

T_2 values are generally much less dependent on field strength, B, than T_1 values.

Hahn echo decay experiment can be used to measure the T_2 time, as shown in the animation below. The size of the echo is recorded for different spacings of the two applied pulses. This reveals the decoherence which is not refocused by the 180° pulse. In simple cases, an exponential decay is measured which is described by the T_2 time.



Spin echo pulse sequence and magnetization decay animation.

T_2* and magnetic field inhomogeneity

In an idealized system, all nuclei in a given chemical environment, in a magnetic field, precess with the same frequency. However, in real systems, there are minor differences in chemical environment which can lead to a distribution of resonance frequencies around the ideal. Over time, this distribution can lead to a dispersion of the tight distribution of magnetic spin vectors, and loss of signal (free induction decay). In fact, for most magnetic resonance experiments, this "relaxation" dominates. This results in dephasing.

However, decoherence because of magnetic field inhomogeneity is not a true "relaxation" process; it is not random, but dependent on the location of the molecule in the magnet. For molecules that aren't moving, the deviation from ideal relaxation is consistent over time, and the signal can be recovered by performing a spin echo experiment.

The corresponding transverse relaxation time constant is thus T_2^*, which is usually much smaller than T_2. The relation between them is:

$$\frac{1}{T_2^*} = \frac{1}{T_2} + \frac{1}{T_{inhom}} = \frac{1}{T_2} + \gamma \Delta B_0$$

where γ represents gyromagnetic ratio, and ΔB_0 the difference in strength of the locally varying field.[5][6]

Unlike T_2, T_2* is influenced by magnetic field gradient irregularities. The T_2* relaxation time is always shorter than the T_2 relaxation time and is typically milliseconds for water samples in imaging magnets.

Is T_1 always longer than T_2?

In NMR systems, the following relation holds absolute true[7] $T_2 \leq 2T_1$. In most situations (but not in principle) T_1 is greater than T_2. The cases in which $2T_1 > T_2 > T_1$ are rare, but not impossible.[8]

Bloch equations

Bloch equations are used to calculate the nuclear magnetization $\mathbf{M} = (M_x, M_y, M_z)$ as a function of time when relaxation times T_1 and T_2 are present. Bloch equations are phenomenological equations that were introduced by Felix Bloch in 1946.[9]

$$\begin{aligned}
\frac{\partial M_x(t)}{\partial t} &= \gamma(\mathbf{M}(t) \times \mathbf{B}(t))_x - \frac{M_x(t)}{T_2} \\
\frac{\partial M_y(t)}{\partial t} &= \gamma(\mathbf{M}(t) \times \mathbf{B}(t))_y - \frac{M_y(t)}{T_2} \\
\frac{\partial M_z(t)}{\partial t} &= \gamma(\mathbf{M}(t) \times \mathbf{B}(t))_z - \frac{M_z(t) - M_0}{T_1}
\end{aligned}$$

Where × is the cross-product, γ is the gyromagnetic ratio and $\mathbf{B}(t) = (B_x(t), B_y(t), B_0 + B_z(t))$ is the magnetic flux density experienced by the nuclei. The z component of the magnetic flux density **B** is typically composed of two terms: one, B_0, is constant in time, the other one, $B_z(t)$, is time dependent. It is present in magnetic resonance imaging and helps with the spatial decoding of the NMR signal.

The equation listed above in the section on T_1 and T_2 relaxation are those in the Bloch equations.

Solomon equations

Solomon equations are used to calculate the transfer of magnetization as a result of relaxation in a dipolar system. They can be employed to explain the nuclear Overhauser effect, which is an important tool in determining molecular structure.

Common relaxation time constants in human tissues

Following is a table of the approximate values of the two relaxation time constants for hydrogen nuclear spins in nonpathological human tissues.

At a main field of 1.5 T

Tissue type	Approximate T_1 value in ms	Approximate T_2 value in ms
Adipose tissues	240-250	60-80
Whole blood (deoxygenated)	1350	50
Whole blood (oxygenated)	1350	200
Cerebrospinal fluid (similar to pure water)	4200 - 4500	2100-2300
Gray matter of cerebrum	920	100
White matter of cerebrum	780	90
Liver	490	40
Kidneys	650	60-75
Muscles	860-900	50

Following is a table of the approximate values of the two relaxation time constants for chemicals that commonly show up in human brain magnetic resonance spectroscopy (MRS) studies, physiologically or pathologically.

At a main field of 1.5 T

Signals of chemical groups	Relative resonance frequency	Approximate T_1 value (ms)	Approximate T_2 value (ms)
Creatine (Cr) and Phosphocreatine (PCr)[10]	3.0 ppm	gray matter: 1150–1340, white matter: 1050–1360	gray matter: 198–207, white matter: 194-218
N-Acetyl group (NA), mainly from N-acetylaspartate (NAA)[10]	2.0 ppm	gray matter: 1170–1370, white matter: 1220-1410	gray matter: 388–426, white matter: 436-519
—CH_3 group of Lactate[11]	1.33 ppm (doublet: 1.27 & 1.39 ppm)	(To be listed)	1040

Relaxation in the rotating frame, $T_{1\rho}$

The discussion above describes relaxation of nuclear magnetization in the presence of a constant magnetic field $\mathbf{B}_0$. This is called **relaxation in the laboratory frame**. Another technique, called **relaxation in the rotating frame**, is the relaxation of nuclear magnetization in the presence of the field $\mathbf{B}_0$ together with a time-dependent magnetic field $\mathbf{B}_1$. The field $\mathbf{B}_1$ rotates in the plane perpendicular to $\mathbf{B}_0$ at the Larmor frequency of the nuclei in the $\mathbf{B}_0$. The magnitude of $\mathbf{B}_1$ is typically much smaller than the magnitude of $\mathbf{B}_0$. Under these circumstances the relaxation of the magnetization is similar to laboratory frame relaxation in a field $\mathbf{B}_1$. The decay constant for the recovery of the magnetization component along $\mathbf{B}_1$ is called the spin-lattice relaxation time in the rotating frame and is denoted $T_{1\rho}$. Relaxation in the rotating frame is useful because it provides information on slow motions of nuclei.

Microscopic mechanisms

Relaxation of nuclear spins requires a microscopic mechanism for a nucleus to change orientation with respect to the applied magnetic field and/or interchange energy with the surroundings (called the lattice). The most common mechanism is the magnetic dipole-dipole interaction between the magnetic moment of a nucleus and the magnetic moment of another nucleus or other entity (electron, atom, ion, molecule). This interaction depends on the distance between the pair of dipoles (spins) but also on their orientation relative to the external magnetic field. Several other relaxation mechanisms also exist. The chemical shift anisotropy (CSA) relaxation mechanism arises whenever the electronic environment around the nucleus is non spherical, the magnitude of the electronic shielding of the nucleus will then be dependent on the molecular orientation relative to the (fixed) external magnetic field. The spin rotation (SR) relaxation mechanism arises from an interaction between the nuclear spin and a coupling to the overall molecular rotational angular momentum. Nuclei with spin $I \geq 1$ will have not only a nuclear dipole but a quadrupole. The nuclear quadrupole has an interaction with the electric field gradient at the nucleus which is again orientation dependent as with the other mechanisms described above, leading to the so-called quadrupolar relaxation mechanism.

Molecular reorientation or tumbling can then modulate these orientation-dependent spin interaction energies. According to quantum mechanics, time-dependent interaction energies cause transitions between the nuclear spin states which result in nuclear spin relaxation. The application of time-dependent perturbation theory in quantum mechanics shows that the relaxation rates (and times) depend on spectral density functions that are the Fourier transforms of the autocorrelation function of the fluctuating magnetic dipole interactions.[12] The form of the spectral density functions depend on the physical system, but a simple approximation called the BPP theory is widely used.

Another relaxation mechanism is the electrostatic interaction between a nucleus with an electric quadrupole moment and the electric field gradient that exists at the nuclear site due to surrounding charges. Thermal motion of a nucleus can result in fluctuating electrostatic interaction energies. These fluctuations produce transitions between the nuclear spin states in a similar manner to the magnetic dipole-dipole interaction.

BPP theory

In 1948, Nicolaas Bloembergen, Edward Mills Purcell, and Robert Pound proposed the so-called Bloembergen-Purcell-Pound theory (BPP theory) to explain the relaxation constant of a pure substance in correspondence with its state, taking into account the effect of tumbling motion of molecules on the local magnetic field disturbance.[13] The theory agrees well with experiments on pure substances, but not for complicated environments such as the human body.

This theory makes the assumption that the autocorrelation function of the microscopic fluctuations causing the relaxation is proportional to e^{-t/τ_c}, where τ_c is called the correlation time. From this theory, one can get $T_1 > T_2$ for magnetic dipolar relaxation:

$$\frac{1}{T_1} = K\left[\frac{\tau_c}{1+\omega_0^2\tau_c^2} + \frac{4\tau_c}{1+4\omega_0^2\tau_c^2}\right]$$
$$\frac{1}{T_2} = \frac{K}{2}\left[3\tau_c + \frac{5\tau_c}{1+\omega_0^2\tau_c^2} + \frac{2\tau_c}{1+4\omega_0^2\tau_c^2}\right],$$

where ω_0 is the Larmor frequency in correspondence with the strength of the main magnetic field B_0. τ_c is the correlation time of the molecular tumbling motion. $K = \frac{3\mu_0^2}{160\pi^2}\frac{\hbar^2\gamma^4}{r^6}$ is defined for spin-1/2 nuclei and is a constant with μ_0 being the magnetic permeability of free space of the $\hbar = \frac{h}{2\pi}$ the reduced Planck constant, γ the gyromagnetic ratio of such species of nuclei, and r the distance between the two nuclei carrying magnetic dipole moment.

Taking for example the H_2O molecules in liquid phase without the contamination of oxygen-17, the value of K is 1.02×10^{10} s^{-2} and the correlation time τ_c is on the order of picoseconds = 10^{-12} s, while hydrogen nuclei ^1H (protons) at 1.5 tesla precess at a Larmor frequency of approximately 64 MHz (Simplified. BPP theory uses angular frequency indeed). We can then estimate using $\tau_c = 5\times10^{-12}$ s:

$$\omega_0\tau_c = 3.2\times10^{-5}\text{(dimensionless)}$$
$$T_1 = \left(1.02\times10^{10}\left[\frac{5\times10^{-12}}{1+(3.2\times10^{-5})^2} + \frac{4\cdot5\times10^{-12}}{1+4\cdot(3.2\times10^{-5})^2}\right]\right)^{-1} = 3.92\text{ s}$$
$$T_2 = \left(\frac{1.02\times10^{10}}{2}\left[3\cdot5\times10^{-12} + \frac{5\cdot5\times10^{-12}}{1+\left(3.2\times10^{-5}\right)^2} + \frac{2\cdot5\times10^{-12}}{1+4\cdot(3.2\times10^{-5})^2}\right]\right)^{-1} = 3.92\text{ s},$$

which is close to the experimental value, 3.6 s. Meanwhile, we can see that at this extreme case, T_1 equals T_2. As follows from the BPP theory, measuring the T_1 times leads to internuclear distances r. One of the examples is accurate determinations of the metal – hydride (M-H) bond lengths in solutions by measurements of ^1H selective and non-selective T_1 times in variable-temperature relaxation experiments via the equation:[14][15]

$$r(M-H) = C\left(\frac{(1.4k+4.47)T_{1min}}{\nu}\right)^{1/6}$$

$k = (f-1)/(0.5-f/3)$, with $f = T_{1s}/T_1$

$$C = 10^7 \left(\frac{\gamma_H^2 \gamma_M^2 \hbar^2 I_M (I_M + 1)}{15} \right)^{1/6}$$

where r, frequency and T_1 are measured in Å, MHz and s, respectively, and I_M is the spin of M.

See also

- Nuclear magnetic resonance
- Nuclear magnetic resonance spectroscopy
- Nuclear magnetic resonance spectroscopy of carbohydrates
- Nuclear magnetic resonance spectroscopy of nucleic acids
- Nuclear magnetic resonance spectroscopy of proteins
- Protein dynamics
- Relaxation (physics)
- Relaxometry
- Spin–lattice relaxation
- Spin–spin relaxation

References

1. Rinck, Peter A. (2022). *Relaxation Times and Basic Pulse Sequences in MR Imaging. in: Magnetic Resonance in Medicine. A Critical Introduction. 12th edition. pp. 65-92* (http://trtf.eu/textbook.htm). Offprint to download: TRTF - The Round Table Foundation / EMRF - European Magnetic Resonance Forum. ISBN 978-3-7460-9518-9.
2. Abragam, A. (1961). "VII Thermal Relaxation in Liquids and Gases". *Principles of Nuclear Magnetism*. Oxford University Press. p. 264. ISBN 019852014X.
3. Hoult, D.I.; Bahkar, B. (1998). "NMR Signal Reception: Virtual Photons and Coherent Spontaneous Emission". *Concepts in Magnetic Resonance*. **9** (5): 277–297. doi:10.1002/(SICI)1099-0534(1997)9:5<277::AID-CMR1>3.0.CO;2-W (https://doi.org/10.1002%2F%28SICI%291099-0534%281997%299%3A5%3C277%3A%3AAID-CMR1%3E3.0.CO%3B2-W).
4. Jarek, Russell L.; Flesher, Robert J.; Shin, Seung Koo (1997). "Kinetics of Internal Rotation of N,N-Dimethylacetamide: A Spin-Saturation Transfer Experiment". *Journal of Chemical Education*. **74** (8): 978. doi:10.1021/ed074p978 (https://doi.org/10.1021%2Fed074p978). ISSN 0021-9584 (https://search.worldcat.org/issn/0021-9584).
5. Chavhan, Govind B; Babyn, Paul S; Thomas, Bejoy; Shroff, Manohar M; Haacke, E. Mark (2009). "Principles, Techniques, and Applications of T2*-based MR Imaging and its Special Applications" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2799958). *Radiographics*. **29** (5): 1433–1449. doi:10.1148/rg.295095034 (https://doi.org/10.1148%2Frg.295095034). PMC 2799958 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2799958). PMID 19755604 (https://pubmed.ncbi.nlm.nih.gov/19755604).
6. "T2* vs T2 relaxation time" (http://mriquestions.com/t2-vs-t2.html). *Questions and Answers in MRI*. Retrieved 2018-08-13.
7. Malcolm H. Levitt: *Spin Dynamics: Basics of Nuclear Magnetic Resonance*, 2nd edition, John Wiley & Sons, New York 2008, ISBN 0-470-51117-6, Section 11.9.2

8. Traficante, Daniel D. (1991). "Relaxation. Can T2, be longer than T1?". *Concepts in Magnetic Resonance*. **3** (3): 171–177. doi:10.1002/cmr.1820030305 (https://doi.org/10.1002%2Fcmr.1820030305).
9. F Bloch, *Nuclear Induction*, Physical Review **70**, 460–473 (1946)
10. **Chemicals of brain relaxation time at 1.5T.** Kreis R, Ernst T, and Ross BD "Absolute Quantification of Water and Metabolites in the Human Brain. II. Metabolite Concentrations" *Journal of Magnetic Resonance*, Series B 102 (1993): 9-19
11. **Lactate relaxation time at 1.5 T**. Isobe T, Matsumura A, Anno I, Kawamura H, Muraishi H, Umeda T, Nose T. "Effect of J coupling and T2 Relaxation in Assessing of Methyl Lactate Signal using PRESS Sequence MR Spectroscopy." *Igaku Butsuri* (2005) v25. 2:68-74.
12. A. Abragam "Principles of Nuclear Magnetism" (Oxford University Press, 1961)
13. Bloembergen, N.; Purcell, E. M.; Pound, R. V. (1948-04-01). "Relaxation Effects in Nuclear Magnetic Resonance Absorption". *Physical Review*. **73** (7): 679–712. doi:10.1103/PhysRev.73.679 (https://doi.org/10.1103%2FPhysRev.73.679). ISSN 0031-899X (https://search.worldcat.org/issn/0031-899X).
14. Gusev, D. G.; Vymenits, A. B.; Bakhmutov, V. I. (1991). "Short spin-lattice relaxation times of hydride ligands. Proton-metal dipole-dipole interactions". *Inorganic Chemistry*. **30** (16): 3116–3118. doi:10.1021/ic00016a003 (https://doi.org/10.1021%2Fic00016a003). ISSN 0020-1669 (https://search.worldcat.org/issn/0020-1669).
15. Gusev, Dmitry G.; Nietlispach, Daniel; Vymenits, Alexey B.; Bakhmutov, Vladimir I.; Berke, Heinz (1993). "Synthesis and NMR T1 relaxation study of rhenium and manganese hydride complexes". *Inorganic Chemistry*. **32** (15): 3270–3276. doi:10.1021/ic00067a013 (https://doi.org/10.1021%2Fic00067a013). ISSN 0020-1669 (https://search.worldcat.org/issn/0020-1669).

External links

- The Basics of NMR (http://www.cis.rit.edu/htbooks/nmr/), RIT
- Relaxation in high-resolution NMR spectroscopy (http://chem.ch.huji.ac.il/nmr/techniques/other/t1t2/t1t2.html)
- Field-cycling NMR relaxometry (http://www.stelar.it/Papers/2004_Kimmich_Nmrd.pdf)
- relax (https://www.nmr-relax.com/) Software for the analysis of NMR dynamics
- Estimation of T1 and T2 relaxation parameters in MRI (https://visielab.uantwerpen.be/sites/default/files/ijist99_0.pdf)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Relaxation_(NMR)&oldid=1230114912"

WIKIPEDIA
The Free Encyclopedia

Spin–lattice relaxation

During nuclear magnetic resonance observations, **spin–lattice relaxation** is the mechanism by which the longitudinal component of the total nuclear magnetic moment vector (parallel to the constant magnetic field) exponentially relaxes from a higher energy, non-equilibrium state to thermodynamic equilibrium with its surroundings (the "lattice"). It is characterized by the **spin–lattice relaxation time**, a time constant known as T_1.

There is a different parameter, T_2, the spin–spin relaxation time, which concerns the exponential relaxation of the transverse component of the nuclear magnetization vector (*perpendicular* to the external magnetic field). Measuring the variation of T_1 and T_2 in different materials is the basis for some magnetic resonance imaging techniques.[1]

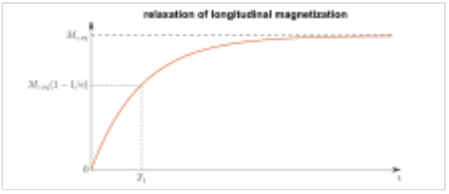
Nuclear physics

T_1 characterizes the rate at which the longitudinal M_z component of the magnetization vector recovers exponentially towards its thermodynamic equilibrium, according to equation

$$M_z(t) = M_{z,\mathrm{eq}} - [M_{z,\mathrm{eq}} - M_z(0)]\, e^{-t/T_1}$$

Or, for the specific case that $M_z(0) = -M_{z,\mathrm{eq}}$

$$M_z(t) = M_{z,\mathrm{eq}} \left(1 - 2e^{-t/T_1}\right)$$



T_1 relaxation or longitudinal relaxation curve

It is thus the time it takes for the longitudinal magnetization to recover approximately 63% [1-(1/e)] of its initial value after being flipped into the magnetic transverse plane by a 90° radiofrequency pulse.

Nuclei are contained within a molecular structure, and are in constant vibrational and rotational motion, creating a complex magnetic field. The magnetic field caused by thermal motion of nuclei within the lattice is called the lattice field. The lattice field of a nucleus in a lower energy state can interact with nuclei in a higher energy state, causing the energy of the higher energy state to distribute itself between the two nuclei. Therefore, the energy gained by nuclei from the RF pulse is dissipated as increased vibration and rotation within the lattice, which can slightly increase the temperature of the sample. The name *spin–lattice relaxation* refers to the process in which the spins give the energy they obtained from the RF pulse back to the surrounding lattice, thereby restoring their equilibrium state. The same process occurs after the spin energy has been altered by a change of the surrounding static magnetic field (e.g. pre-polarization by or insertion into high magnetic field) or if the nonequilibrium state has been achieved by other means (e.g., hyperpolarization by optical pumping).

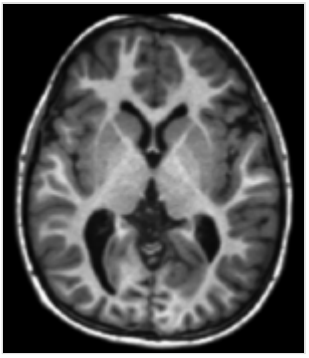
The relaxation time, T_1 (the average lifetime of nuclei in the higher energy state) is dependent on the gyromagnetic ratio of the nucleus and the mobility of the lattice. As mobility increases, the vibrational and rotational frequencies increase, making it more likely for a component of the lattice field to be able to

stimulate the transition from high to low energy states. However, at extremely high mobilities, the probability decreases as the vibrational and rotational frequencies no longer correspond to the energy gap between states.

Different tissues have different T_1 values. For example, fluids have long T_1s (1500-2000 ms), and water-based tissues are in the 400-1200 ms range, while fat based tissues are in the shorter 100-150 ms range. The presence of strongly magnetic ions or particles (e.g., ferromagnetic or paramagnetic) also strongly alter T_1 values and are widely used as MRI contrast agents.

T_1 weighted images

Magnetic resonance imaging uses the resonance of the protons to generate images. Protons are excited by a radio frequency pulse at an appropriate frequency (Larmor frequency) and then the excess energy is released in the form of a minuscule amount of heat to the surroundings as the spins return to their thermal equilibrium. The magnetization of the proton ensemble goes back to its equilibrium value with an exponential curve characterized by a time constant T_1 (see Relaxation (NMR)).



A T_1 weighted image of the head.

T_1 weighted images can be obtained by setting short repetition time (TR) such as < 750 ms and echo time (TE) such as < 40 ms in conventional spin echo sequences, while in Gradient Echo Sequences they can be obtained by using flip angles of larger than 50^o while setting TE values to less than 15 ms.

T_1 is significantly different between grey matter and white matter and is used when undertaking brain scans. A strong T_1 contrast is present between fluid and more solid anatomical structures, making T_1 contrast suitable for morphological assessment of the normal or pathological anatomy, e.g., for musculoskeletal applications.

In the rotating frame

Spin–lattice relaxation in the rotating frame is the mechanism by which M_{xy}, the transverse component of the magnetization vector, exponentially decays towards its equilibrium value of zero, under the influence of a radio frequency (RF) field in nuclear magnetic resonance (NMR) and magnetic resonance imaging (MRI). It is characterized by the spin–lattice relaxation **time constant** in the rotating frame, $T_{1\rho}$. It is named in contrast to T_1, the spin-lattice relaxation time.[2]

$T_{1\rho}$ MRI is an alternative to conventional T_1 and T_2 MRI by its use of a long-duration, low-power radio frequency referred to as spin-lock (SL) pulse applied to the magnetization in the transverse plane. The magnetization is effectively spin-locked around an effective B_1 field created by the vector sum of the applied B_1 and any off-resonant component. The spin-locked magnetization will relax with a time

constant $T_{1\rho}$, which is the time it takes for the magnetic resonance signal to reach 37% (1/e) of its initial value, $M_{xy}(0)$. Hence the relation: $M_{xy}(t_{\mathrm{SL}}) = M_{xy}(0)e^{-t_{\mathrm{SL}}/T_{1\rho}}$, where t_{SL} is the duration of the RF field.

Measurement

$T_{1\rho}$ can be quantified (relaxometry) by curve fitting the signal expression above as a function of the duration of the spin-lock pulse while the amplitude of spin-lock pulse (γB_1~0.1-few kHz) is fixed. Quantitative $T_{1\rho}$ MRI relaxation maps reflect the biochemical composition of tissues.[3]

Imaging

$T_{1\rho}$ MRI has been used to image tissues such as cartilage,[4][5] intervertebral discs,[6] brain,[7][8] and heart,[9] as well as certain types of cancers.[10][11]

See also

- Relaxation (NMR)
- Spin–spin relaxation time
- Ernst angle

References

1. Rinck, Peter A. (2022). *Relaxation Times and Basic Pulse Sequences in MR Imaging. in: Magnetic Resonance in Medicine. A Critical Introduction. 12th edition. pp. 65-92* (http://trtf.eu/textbook.htm). Offprint to download: TRTF - The Round Table Foundation / EMRF - European Magnetic Resonance Forum. ISBN 978-3-7460-9518-9.
2. Levitt, Malcolm H. (2016). *Spin Dynamics: Basics of Nuclear Magnetic Resonance 2nd Edition*. Wiley. ISBN 978-0470511176.
3. Borthakur, A; Mellon, E; Niyogi, S; Witschey, W; Kneeland, JB; Reddy, R (Nov 2006). "Sodium and T1rho MRI for molecular and diagnostic imaging of articular cartilage" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2896046). *NMR in Biomedicine*. **19** (7): 781–821. doi:10.1002/nbm.1102 (https://doi.org/10.1002%2Fnbm.1102). PMC 2896046 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2896046). PMID 17075961 (https://pubmed.ncbi.nlm.nih.gov/17075961).
4. Li, X; Benjamin Ma, C; Link, TM; Castillo, DD; Blumenkrantz, G; Lozano, J; Carballido-Gamio, J; Ries, M; Majumdar, S (Jul 2007). "In vivo T(1rho) and T(2) mapping of articular cartilage in osteoarthritis of the knee using 3 T MRI" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2040334). *Osteoarthritis and Cartilage*. **15** (7): 789–97. doi:10.1016/j.joca.2007.01.011 (https://doi.org/10.1016%2Fj.joca.2007.01.011). PMC 2040334 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2040334). PMID 17307365 (https://pubmed.ncbi.nlm.nih.gov/17307365).
5. Witschey, WR; Borthakur, A; Fenty, M; Kneeland, BJ; Lonner, JH; McArdle, EL; Sochor, M; Reddy, R (May 2010). "T1rho MRI quantification of arthroscopically confirmed cartilage degeneration" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2933515). *Magnetic Resonance in Medicine*. **63** (5): 1376–82. doi:10.1002/mrm.22272 (https://doi.org/10.1002%2Fmrm.22272). PMC 2933515 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2933515). PMID 20432308 (https://pubmed.ncbi.nlm.nih.gov/20432308).

6. Borthakur, A; Maurer, PM; Fenty, M; Wang, C; Berger, R; Yoder, J; Balderston, RA; Elliott, DM (Dec 1, 2011). "T1ρ magnetic resonance imaging and discography pressure as novel biomarkers for disc degeneration and low back pain" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4002043). *Spine*. **36** (25): 2190–6. doi:10.1097/BRS.0b013e31820287bf (https://doi.org/10.1097%2FBRS.0b013e31820287bf). PMC 4002043 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4002043). PMID 21358489 (https://pubmed.ncbi.nlm.nih.gov/21358489).
7. Borthakur, A; Sochor, M; Davatzikos, C; Trojanowski, JQ; Clark, CM (Jul 15, 2008). "T1rho MRI of Alzheimer's disease" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2473861). *NeuroImage*. **41** (4): 1199–205. doi:10.1016/j.neuroimage.2008.03.030 (https://doi.org/10.1016%2Fj.neuroimage.2008.03.030). PMC 2473861 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2473861). PMID 18479942 (https://pubmed.ncbi.nlm.nih.gov/18479942).
8. Cai, K; Haris, M; Singh, A; Kogan, F; Greenberg, JH; Hariharan, H; Detre, JA; Reddy, R (Jan 22, 2012). "Magnetic resonance imaging of glutamate" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3274604). *Nature Medicine*. **18** (2): 302–6. doi:10.1038/nm.2615 (https://doi.org/10.1038%2Fnm.2615). PMC 3274604 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3274604). PMID 22270722 (https://pubmed.ncbi.nlm.nih.gov/22270722).
9. Witschey, WR; Pilla, JJ; Ferrari, G; Koomalsingh, K; Haris, M; Hinmon, R; Zsido, G; Gorman JH, 3rd; Gorman, RC; Reddy, R (Nov 2010). "Rotating frame spin lattice relaxation in a swine model of chronic, left ventricular myocardial infarction" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2965811). *Magnetic Resonance in Medicine*. **64** (5): 1453–60. doi:10.1002/mrm.22543 (https://doi.org/10.1002%2Fmrm.22543). PMC 2965811 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2965811). PMID 20677236 (https://pubmed.ncbi.nlm.nih.gov/20677236).
10. Li, LZ; Zhou, R; Xu, HN; Moon, L; Zhong, T; Kim, EJ; Qiao, H; Reddy, R; Leeper, D; Chance, B; Glickson, JD (Apr 21, 2009). "Quantitative magnetic resonance and optical imaging biomarkers of melanoma metastatic potential" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2672511). *Proceedings of the National Academy of Sciences of the United States of America*. **106** (16): 6608–13. Bibcode:2009PNAS..106.6608L (https://ui.adsabs.harvard.edu/abs/2009PNAS..106.6608L). doi:10.1073/pnas.0901807106 (https://doi.org/10.1073%2Fpnas.0901807106). PMC 2672511 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2672511). PMID 19366661 (https://pubmed.ncbi.nlm.nih.gov/19366661).
11. Cai, K; Shore, A; Singh, A; Haris, M; Hiraki, T; Waghray, P; Reddy, D; Greenberg, JH; Reddy, R (Feb 2, 2012). "Blood oxygen level dependent angiography (BOLDangio) and its potential applications in cancer research" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3390450). *NMR in Biomedicine*. **25** (10): 1125–1132. doi:10.1002/nbm.2780 (https://doi.org/10.1002%2Fnbm.2780). PMC 3390450 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3390450). PMID 22302557 (https://pubmed.ncbi.nlm.nih.gov/22302557).

Further reading

- McRobbie D., et al. *MRI, From picture to proton.* 2003
- Hashemi Ray, et al. *MRI, The Basics* 2ED. 2004

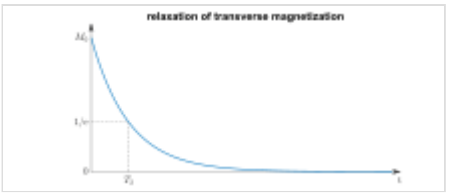
Retrieved from "https://en.wikipedia.org/w/index.php?title=Spin–lattice_relaxation&oldid=1225951316"

WIKIPEDIA
The Free Encyclopedia

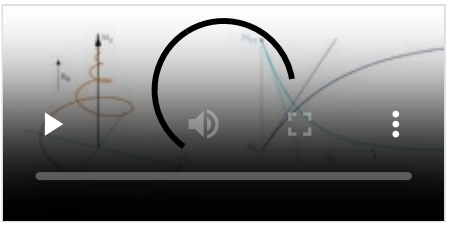
Spin–spin relaxation

In physics, the **spin–spin relaxation** is the mechanism by which M_{xy}, the transverse component of the magnetization vector, exponentially decays towards its equilibrium value in nuclear magnetic resonance (NMR) and magnetic resonance imaging (MRI). It is characterized by the **spin–spin relaxation time**, known as $\boldsymbol{T_2}$, a time constant characterizing the signal decay.[1] [2] [3] It is named in contrast to T_1, the spin–lattice relaxation time. It is the time it takes for the magnetic resonance signal to irreversibly decay to 37% (1/e) of its initial value after its generation by tipping the longitudinal magnetization towards the magnetic transverse plane.[4] Hence the relation

$$\boldsymbol{M_{xy}(t) = M_{xy}(0)e^{-t/T_2}} \ .$$



T_2 relaxation curve


Visualization of the $\boldsymbol{T_1}$ and $\boldsymbol{T_2}$ relaxation times.

T_2 relaxation generally proceeds more rapidly than T_1 recovery, and different samples and different biological tissues have different T_2. For example, fluids have the longest T_2, and water based tissues are in the 40–200 ms range, while fat based tissues are in the 10–100 ms range. Amorphous solids have T_2 in the range of milliseconds, while the transverse magnetization of crystalline samples decays in around 1/20 ms.

Origin

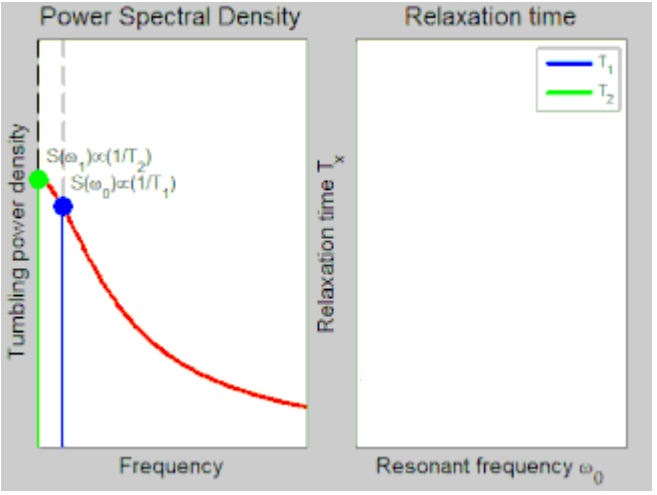
When excited nuclear spins—i.e., those lying partially in the transverse plane—interact with each other by sampling local magnetic field inhomogeneities on the micro- and nanoscales, their respective accumulated phases deviate from expected values.[4] While the slow- or non-varying component of this deviation is reversible, some net signal will inevitably be lost due to short-lived interactions such as collisions and random processes such as diffusion through heterogeneous space.

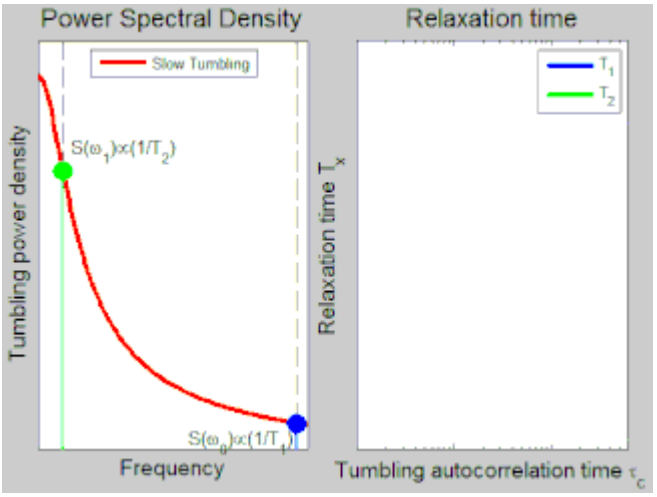
T_2 decay does not occur due to the tilting of the magnetization vector away from the transverse plane. Rather, it is observed due to the interactions of an ensemble of spins dephasing from each other.[5] Unlike spin-lattice relaxation, considering spin-spin relaxation using only a single isochromat is trivial and not informative.

Determining parameters

Like spin-lattice relaxation, spin-spin relaxation can be studied using a molecular tumbling autocorrelation framework.[6] The resulting signal decays exponentially as the echo time (TE), i.e., the time after excitation at which readout occurs, increases. In more complicated experiments, multiple echoes can be acquired simultaneously in order to quantitatively evaluate one or more superimposed T_2 decay curves.[6] The relaxation rate experienced by a spin, which is the inverse of T_2, is proportional to a

spin's tumbling energy at the frequency *difference* between one spin and another; in less mathematical terms, energy is transferred between two spins when they rotate at a similar frequency to their beat frequency, ω_1 in the figure at right.[6] In that the beat frequency range is very small relative to the average rotation rate $(1/\tau_c)$, spin-spin relaxation is not heavily dependent on magnetic field strength. This directly contrasts with spin-lattice relaxation, which occurs at tumbling frequencies equal to the Larmor frequency ω_0.[7] Some frequency shifts, such as the NMR chemical shift, occur at frequencies proportional to the Larmor frequency, and the related but distinct parameter T_2^* can be heavily dependent on field strength due to the difficulty of correcting for inhomogeneity in stronger magnet bores.[4]





Assuming isothermal conditions, spins tumbling faster through space will generally have a longer T_2. Since slower tumbling displaces the spectral energy at high tumbling frequencies to lower frequencies, the relatively low beat frequency will experience a monotonically increasing amount of energy as τ_c increases, decreasing relaxation time.[6] The figure at the left illustrates this relationship. It is worth noting again that fast tumbling spins, such as those in pure water, have similar T_1 and T_2 relaxation times,[6] while slow tumbling spins, such as those in crystal lattices, have very distinct relaxation times.

Measurement

A spin echo experiment can be used to reverse time-invariant dephasing phenomena such as millimeter-scale magnetic inhomogeneities.[6] The resulting signal decays exponentially as the echo time (TE), i.e., the time after excitation at which readout occurs, increases. In more complicated experiments, multiple echoes can be acquired simultaneously in order to quantitatively evaluate one or more superimposed T_2 decay curves.[6] In MRI, T_2-weighted images can be obtained by selecting an echo time on the order of the various tissues' T_2s.[8] In order to reduce the amount of T_1 information and therefore contamination in the image, excited spins are allowed to return to near-equilibrium on a T_1 scale before being excited again. (In MRI parlance, this waiting time is called the "repetition time" and is abbreviated TR). Pulse

sequences other than the conventional spin echo can also be used to measure T_2; gradient echo sequences such as steady-state free precession (SSFP) and multiple spin echo sequences can be used to accelerate image acquisition or inform on additional parameters.[6][8]

See also

- Relaxation (NMR)
- Spin–lattice relaxation
- Spin echo

References

1. Abragam, A. (1961). *Principles of Nuclear Magnetism*. Clarendon Press. p. 15. ISBN 019852014X.
2. Claridge, Timothy D.W. (2016). *High Resolution NMR Techniques in Organic Chemistry, 3rd ed*. Elsevier. p. 26-30. ISBN 978-0080999869.
3. Levitt, Malcolm H. (2016). *Spin Dynamics: Basics of Nuclear Magnetic Resonance 2nd Edition*. Wiley. ISBN 978-0470511176.
4. Chavhan, Govind; Babyn, Paul; Thomas, Bejoy; Shroff, Manohar; Haacke, Mark (September 2009). "Principles, Techniques, and Applications of T2*-based MR Imaging and Its Special Applications" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2799958). *RadioGraphics*. **29** (5): 1433–1449. doi:10.1148/rg.295095034 (https://doi.org/10.1148%2Frg.295095034). PMC 2799958 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2799958). PMID 19755604 (https://pubmed.ncbi.nlm.nih.gov/19755604).
5. Becker, Edwin (October 1999). *High Resolution NMR* (https://www.sciencedirect.com/book/9780120846627/high-resolution-nmr#book-info) (3rd ed.). San Diego, California: Academic Press. p. 209. ISBN 978-0-12-084662-7. Retrieved 8 May 2019.
6. Becker, Edwin (October 1999). *High Resolution NMR* (https://www.sciencedirect.com/book/9780120846627/high-resolution-nmr#book-info) (3rd ed.). San Diego, California: Academic Press. p. 228. ISBN 978-0-12-084662-7. Retrieved 8 May 2019.
7. Yury, Shapiro (September 2011). "Structure and dynamics of hydrogels and organogels: An NMR spectroscopy approach". *Progress in Polymer Science*. **36** (9): 1184–1253. doi:10.1016/j.progpolymsci.2011.04.002 (https://doi.org/10.1016%2Fj.progpolymsci.2011.04.002).
8. Basser, Peter; Mattiello, James; LeBihan, Denis (January 1994). "MR diffusion tensor spectroscopy and imaging" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1275686). *Biophysical Journal*. **66** (1): 259–267. Bibcode:1994BpJ....66..259B (https://ui.adsabs.harvard.edu/abs/1994BpJ....66..259B). doi:10.1016/S0006-3495(94)80775-1 (https://doi.org/10.1016%2FS0006-3495%2894%2980775-1). PMC 1275686 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1275686). PMID 8130344 (https://pubmed.ncbi.nlm.nih.gov/8130344).

- Ray Freeman (1999). *Spin Choreography: Basic Steps in High Resolution NMR*. Oxford University Press. ISBN 978-0-19-850481-8.
- Malcolm H. Levitt (2001). *Spin Dynamics: Basics of Nuclear Magnetic Resonance* (https://archive.org/details/isbn_9780471489221). Wiley. ISBN 978-0-471-48922-1.
- Arthur Schweiger; Gunnar Jeschke (2001). *Principles of Pulse Electron Paramagnetic Resonance*. Oxford University Press. ISBN 978-0-19-850634-8.

- McRobbie D., et al. *MRI, From picture to proton.* 2003
- Hashemi Ray, et al. *MRI, The Basics* 2ED. 2004.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Spin–spin_relaxation&oldid=1222802668"

WIKIPEDIA
The Free Encyclopedia

Model of computation

In computer science, and more specifically in computability theory and computational complexity theory, a **model of computation** is a model which describes how an output of a mathematical function is computed given an input. A model describes how units of computations, memories, and communications are organized.[1] The computational complexity of an algorithm can be measured given a model of computation. Using a model allows studying the performance of algorithms independently of the variations that are specific to particular implementations and specific technology.

Models

Models of computation can be classified into three categories: sequential models, functional models, and concurrent models.

Sequential models

Sequential models include:

- Finite state machines
- Post machines (Post–Turing machines and tag machines).
- Pushdown automata
- Register machines
  - Random-access machines
- Turing machines
- Decision tree model

Functional models

Functional models include:

- Abstract rewriting systems
- Combinatory logic
- General recursive functions
- Lambda calculus

Concurrent models

Concurrent models include:

- Actor model
- Cellular automaton
- Interaction nets
- Kahn process networks

- Logic gates and digital circuits
- Petri nets
- Process calculus
- Synchronous Data Flow

Some of these models have both deterministic and nondeterministic variants. Nondeterministic models correspond to limits of certain sequences of finite computers, but do not correspond to any subset of finite computers; they are used in the study of computational complexity of algorithms.

Models differ in their expressive power; for example, each function that can be computed by a *Finite state machine* can also be computed by a *Turing machine*, but not vice versa.

Uses

In the field of runtime analysis of algorithms, it is common to specify a computational model in terms of *primitive operations* allowed which have unit cost, or simply **unit-cost operations**. A commonly used example is the random-access machine, which has unit cost for read and write access to all of its memory cells. In this respect, it differs from the above-mentioned Turing machine model.

See also

- Stack machine (0-operand machine)
- Accumulator machine (1-operand machine)
- Register machine (2,3,... operand machine)
- Random-access machine
- Abstract machine
- Cell-probe model
- Robertson–Webb query model
- Chomsky hierarchy
- Turing completeness

References

1. "Models of Computation" (https://cs.brown.edu/people/jsavage/book/pdfs/ModelsOfComputation.pdf) (PDF).

Further reading

- Fernández, Maribel (2009). *Models of Computation: An Introduction to Computability Theory*. Undergraduate Topics in Computer Science. Springer. ISBN 978-1-84882-433-1.
- Savage, John E. (1998). *Models Of Computation: Exploring the Power of Computing*. Addison-Wesley. ISBN 978-0201895391.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Model_of_computation&oldid=1243830299"

WIKIPEDIA
The Free Encyclopedia

Adiabatic quantum computation

Adiabatic quantum computation (**AQC**) is a form of quantum computing which relies on the adiabatic theorem to perform calculations[1] and is closely related to quantum annealing.[2][3][4][5]

Description

First, a (potentially complicated) Hamiltonian is found whose ground state describes the solution to the problem of interest. Next, a system with a simple Hamiltonian is prepared and initialized to the ground state. Finally, the simple Hamiltonian is adiabatically evolved to the desired complicated Hamiltonian. By the adiabatic theorem, the system remains in the ground state, so at the end, the state of the system describes the solution to the problem. Adiabatic quantum computing has been shown to be polynomially equivalent to conventional quantum computing in the circuit model.[6]

The time complexity for an adiabatic algorithm is the time taken to complete the adiabatic evolution which is dependent on the gap in the energy eigenvalues (spectral gap) of the Hamiltonian. Specifically, if the system is to be kept in the ground state, the energy gap between the ground state and the first excited state of $H(t)$ provides an upper bound on the rate at which the Hamiltonian can be evolved at time t.[7] When the spectral gap is small, the Hamiltonian has to be evolved slowly. The runtime for the entire algorithm can be bounded by:

$$T = O\left(\frac{1}{g_{min}^2}\right)$$

where g_{min} is the minimum spectral gap for $H(t)$.

AQC is a possible method to get around the problem of energy relaxation. Since the quantum system is in the ground state, interference with the outside world cannot make it move to a lower state. If the energy of the outside world (that is, the "temperature of the bath") is kept lower than the energy gap between the ground state and the next higher energy state, the system has a proportionally lower probability of going to a higher energy state. Thus the system can stay in a single system eigenstate as long as needed.

Universality results in the adiabatic model are tied to quantum complexity and QMA-hard problems. The k-local Hamiltonian is QMA-complete for k ≥ 2.[8] QMA-hardness results are known for physically realistic lattice models of qubits such as[9]

$$H = \sum_i h_i Z_i + \sum_{i<j} J^{ij} Z_i Z_j + \sum_{i<j} K^{ij} X_i X_j$$

where Z, X represent the Pauli matrices σ_z, σ_x. Such models are used for universal adiabatic quantum computation. The Hamiltonians for the QMA-complete problem can also be restricted to act on a two dimensional grid of qubits[10] or a line of quantum particles with 12 states per particle.[11] If such models

were found to be physically realizable, they too could be used to form the building blocks of a universal adiabatic quantum computer.

In practice, there are problems during a computation. As the Hamiltonian is gradually changed, the interesting parts (quantum behavior as opposed to classical) occur when multiple qubits are close to a tipping point. It is exactly at this point when the ground state (one set of qubit orientations) gets very close to a first energy state (a different arrangement of orientations). Adding a slight amount of energy (from the external bath, or as a result of slowly changing the Hamiltonian) could take the system out of the ground state, and ruin the calculation. Trying to perform the calculation more quickly increases the external energy; scaling the number of qubits makes the energy gap at the tipping points smaller.

Adiabatic quantum computation in satisfiability problems

Adiabatic quantum computation solves satisfiability problems and other combinatorial search problems. Specifically, these kind of problems seek a state that satisfies $C_1 \wedge C_2 \wedge \cdots \wedge C_M$. This expression contains the satisfiability of M clauses, for which clause C_i has the value True or False, and can involve n bits. Each bit is a variable $x_j \in \{0,1\}$ such that C_i is a Boolean value function of $x_1, x_2, \ldots, x_n$. QAA solves this kind of problem using quantum adiabatic evolution. It starts with an Initial Hamiltonian H_B:

$$H_B = H_{B_1} + H_{B_2} + \cdots + H_{B_M}$$

where H_{B_i} shows the Hamiltonian corresponding to the clause C_i. Usually, the choice of H_{B_i} won't depend on different clauses, so only the total number of times each bit is involved in all clauses matters. Next, it goes through an adiabatic evolution, ending in the Problem Hamiltonian H_P:

$$H_P = \sum_C H_{P,C}$$

where $H_{P,C}$ is the satisfying Hamiltonian of clause C.

It has eigenvalues:

$$h_C(z_{1C}, z_{2C} \ldots z_{nC}) = \begin{cases} 0 & \text{clause } C \text{ satisfied} \\ 1 & \text{clause } C \text{ violated} \end{cases}$$

For a simple path of adiabatic evolution with run time T, consider:

$$H(t) = (1 - t/T)H_B + (t/T)H_P$$

and let $s = t/T$. This results in:

$\tilde{H}(s) = (1 - s)H_B + sH_P$, which is the adiabatic evolution Hamiltonian of the algorithm.

In accordance with the adiabatic theorem, start from the ground state of Hamiltonian H_B at the beginning, proceed through an adiabatic process, and end in the ground state of problem Hamiltonian H_P .

Then measure the z-component of each of the n spins in the final state. This will produce a string $z_1, z_2, \ldots, z_n$ which is highly likely to be the result of the satisfiability problem. The run time T must be sufficiently long to assure correctness of the result. According to the adiabatic theorem, T is about $\varepsilon / g_{\min}^2$, where $g_{\min} = \min_{0 \le s \le 1} \left(E_1(s) - E_0(s) \right)$ is the minimum energy gap between ground state and first excited state.[12]

Comparison to gate-based quantum computing

Adiabatic quantum computing is equivalent in power to standard gate-based quantum computing that implements arbitrary unitary operations. However, the mapping challenge on gate-based quantum devices differs substantially from quantum annealers as logical variables are mapped only to single qubits and not to chains.[13]

D-Wave quantum processors

The D-Wave One is a device made by Canadian company D-Wave Systems, which claims that it uses quantum annealing to solve optimization problems.[14][15] On 25 May 2011, Lockheed-Martin purchased a D-Wave One for about US$10 million.[15] In May 2013, Google purchased a 512 qubit D-Wave Two.[16]

The question of whether the D-Wave processors offer a speedup over a classical processor is still unanswered. Tests performed by researchers at Quantum Artificial Intelligence Lab (NASA), USC, ETH Zurich, and Google show that as of 2015, there is no evidence of a quantum advantage.[17][18][19]

Notes

1. Farhi, E.; Goldstone, Jeffrey; Gutmann, S.; Sipser, M. (2000). "Quantum Computation by Adiabatic Evolution". arXiv:quant-ph/0001106v1 (https://arxiv.org/abs/quant-ph/0001106v1).
2. Kadowaki, T.; Nishimori, H. (November 1, 1998). "Quantum annealing in the transverse Ising model". *Physical Review E*. **58** (5): 5355. arXiv:cond-mat/9804280 (https://arxiv.org/abs/cond-mat/9804280). Bibcode:1998PhRvE..58.5355K (https://ui.adsabs.harvard.edu/abs/1998PhRvE..58.5355K). doi:10.1103/PhysRevE.58.5355 (https://doi.org/10.1103%2FPhysRevE.58.5355). S2CID 36114913 (https://api.semanticscholar.org/CorpusID:36114913).
3. Finilla, A. B.; Gomez, M. A.; Sebenik, C.; Doll, D. J. (March 18, 1994). "Quantum annealing: A new method for minimizing multidimensional functions". *Chemical Physics Letters*. **219** (5): 343–348. arXiv:chem-ph/9404003 (https://arxiv.org/abs/chem-ph/9404003). Bibcode:1994CPL...219..343F (https://ui.adsabs.harvard.edu/abs/1994CPL...219..343F). doi:10.1016/0009-2614(94)00117-0 (https://doi.org/10.1016%2F0009-2614%2894%2900117-0). S2CID 97302385 (https://api.semanticscholar.org/CorpusID:97302385).
4. Santoro, G. E.; Tosatti, E. (September 8, 2006). "Optimization using quantum mechanics: quantum annealing through adiabatic evolution". *Journal of Physics A*. **39** (36): R393. Bibcode:2006JPhA...39R.393S (https://ui.adsabs.harvard.edu/abs/2006JPhA...39R.393S). doi:10.1088/0305-4470/39/36/R01 (https://doi.org/10.1088%2F0305-4470%2F39%2F36%2FR01). S2CID 116931586 (https://api.semanticscholar.org/CorpusID:116931586).

5. Das, A.; Chakrabarti, B. K. (September 5, 2008). "Colloquium: Quantum annealing and analog quantum computation". *Reviews of Modern Physics*. **80** (3): 1061. arXiv:0801.2193 (https://arxiv.org/abs/0801.2193). Bibcode:2008RvMP...80.1061D (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1061D). doi:10.1103/RevModPhys.80.1061 (https://doi.org/10.1103%2FRevModPhys.80.1061). S2CID 14255125 (https://api.semanticscholar.org/CorpusID:14255125).
6. Aharonov, Dorit; van Dam, Wim; Kempe, Julia; Landau, Zeph; LLoyd, Seth (April 1, 2007). "Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation". *SIAM Journal on Computing*. **37**: 166. arXiv:quant-ph/0405098 (https://arxiv.org/abs/quant-ph/0405098). doi:10.1137/s0097539705447323 (https://doi.org/10.1137%2Fs0097539705447323).
7. van Dam, Wim; van Mosca, Michele; Vazirani, Umesh. "How Powerful is Adiabatic Quantum Computation?". *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*: 279.
8. Kempe, J.; Kitaev, A.; Regev, O. (July 27, 2006). "The Complexity of the Local Hamiltonian Problem". *SIAM Journal on Computing*. **35** (5): 1070–1097. arXiv:quant-ph/0406180v2 (https://arxiv.org/abs/quant-ph/0406180v2). doi:10.1137/S0097539704445226 (https://doi.org/10.1137%2FS0097539704445226). ISSN 1095-7111 (https://search.worldcat.org/issn/1095-7111).
9. Biamonte, J. D.; Love, P. J. (July 28, 2008). "Realizable Hamiltonians for Universal Adiabatic Quantum Computers". *Physical Review A*. **78** (1): 012352. arXiv:0704.1287 (https://arxiv.org/abs/0704.1287). Bibcode:2008PhRvA..78a2352B (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78a2352B). doi:10.1103/PhysRevA.78.012352 (https://doi.org/10.1103%2FPhysRevA.78.012352). S2CID 9859204 (https://api.semanticscholar.org/CorpusID:9859204).
10. Oliveira, R.; Terhal, B. M. (November 1, 2008). "The complexity of quantum spin systems on a two-dimensional square lattice". *Quantum Information & Computation*. **8** (10): 0900–0924. arXiv:quant-ph/0504050 (https://arxiv.org/abs/quant-ph/0504050). Bibcode:2005quant.ph..4050O (https://ui.adsabs.harvard.edu/abs/2005quant.ph..4050O). doi:10.26421/QIC8.10-2 (https://doi.org/10.26421%2FQIC8.10-2). S2CID 3262293 (https://api.semanticscholar.org/CorpusID:3262293).
11. Aharonov, D.; Gottesman, D.; Irani, S.; Kempe, J. (April 1, 2009). "The Power of Quantum Systems on a Line". *Communications in Mathematical Physics*. **287** (1): 41–65. arXiv:0705.4077 (https://arxiv.org/abs/0705.4077). Bibcode:2009CMaPh.287...41A (https://ui.adsabs.harvard.edu/abs/2009CMaPh.287...41A). doi:10.1007/s00220-008-0710-3 (https://doi.org/10.1007%2Fs00220-008-0710-3). S2CID 1916001 (https://api.semanticscholar.org/CorpusID:1916001).
12. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam; Sipser, Michael (January 28, 2000). "Quantum Computation by Adiabatic Evolution". arXiv:quant-ph/0001106 (https://arxiv.org/abs/quant-ph/0001106).
13. Zbinden, Stefanie (June 15, 2020). "Embedding Algorithms for Quantum Annealers with Chimera and Pegasus Connection Topologies". *High Performance Computing*. Lecture Notes in Computer Science. Vol. 12151. pp. 187–206. doi:10.1007/978-3-030-50743-5_10 (https://doi.org/10.1007%2F978-3-030-50743-5_10). ISBN 978-3-030-50742-8.
14. Johnson, M.; Amin, M. (May 11, 2011). "Quantum annealing with manufactured spins" (https://www.nature.com/articles/nature10012). *Nature*. **473** (7346): 194–198. Bibcode:2011Natur.473..194J (https://ui.adsabs.harvard.edu/abs/2011Natur.473..194J). doi:10.1038/nature10012 (https://doi.org/10.1038%2Fnature10012). PMID 21562559 (https://pubmed.ncbi.nlm.nih.gov/21562559). S2CID 205224761 (https://api.semanticscholar.org/CorpusID:205224761). Retrieved February 12, 2021. "Some of the authors are employees of D-Wave Systems Inc."
15. Campbell, Macgregor (June 1, 2011). "Quantum computer sold to high-profile client" (https://www.newscientist.com/article/dn20529-quantum-computer-sold-to-high-profile-client/). *New Scientist*. Retrieved February 12, 2021.

16. Jones, Nicola (June 20, 2013). "Computing: The quantum company" (https://doi.org/10.1038%2F498286a). *Nature*. **498** (7454): 286–288. Bibcode:2013Natur.498..286J (https://ui.adsabs.harvard.edu/abs/2013Natur.498..286J). doi:10.1038/498286a (https://doi.org/10.1038%2F498286a). PMID 23783610 (https://pubmed.ncbi.nlm.nih.gov/23783610).
17. Boixo, S.; Rønnow, T. F.; Isakov, S. V.; Wang, Z.; Wecker, D.; Lidar, D. A.; Martinis, J. M.; Troyer, M. (February 28, 2014). "Evidence for quantum annealing with more than one hundred qubits". *Nature Physics*. **10** (3): 218–224. arXiv:1304.4595 (https://arxiv.org/abs/1304.4595). Bibcode:2014NatPh..10..218B (https://ui.adsabs.harvard.edu/abs/2014NatPh..10..218B). doi:10.1038/nphys2900 (https://doi.org/10.1038%2Fnphys2900). S2CID 8031023 (https://api.semanticscholar.org/CorpusID:8031023).
18. Ronnow, T. F.; Wang, Z.; Job, J.; Boixo, S.; Isakov, S. V.; Wecker, D.; Martinis, J. M.; Lidar, D. A.; Troyer, M. (July 25, 2014). "Defining and detecting quantum speedup". *Science*. **345** (6195): 420–424. arXiv:1401.2910 (https://arxiv.org/abs/1401.2910). Bibcode:2014Sci...345..420R (https://ui.adsabs.harvard.edu/abs/2014Sci...345..420R). doi:10.1126/science.1252319 (https://doi.org/10.1126%2Fscience.1252319). PMID 25061205 (https://pubmed.ncbi.nlm.nih.gov/25061205). S2CID 5596838 (https://api.semanticscholar.org/CorpusID:5596838).
19. Venturelli, D.; Mandrà, S.; Knysh, S.; O'Gorman, B.; Biswas, R.; Smelyanskiy, V. (September 18, 2015). "Quantum Optimization of Fully Connected Spin Glasses". *Physical Review X*. **5** (3): 031040. arXiv:1406.7553 (https://arxiv.org/abs/1406.7553). Bibcode:2015PhRvX...5c1040V (https://ui.adsabs.harvard.edu/abs/2015PhRvX...5c1040V). doi:10.1103/PhysRevX.5.031040 (https://doi.org/10.1103%2FPhysRevX.5.031040). S2CID 118622447 (https://api.semanticscholar.org/CorpusID:118622447).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Adiabatic_quantum_computation&oldid=1174798482"

WIKIPEDIA
The Free Encyclopedia

Continuous-variable quantum information

Continuous-variable (**CV**) **quantum information** is the area of quantum information science that makes use of physical observables, like the strength of an electromagnetic field, whose numerical values belong to continuous intervals.[1][2][3] One primary application is quantum computing. In a sense, continuous-variable quantum computation is "analog", while quantum computation using qubits is "digital." In more technical terms, the former makes use of Hilbert spaces that are infinite-dimensional, while the Hilbert spaces for systems comprising collections of qubits are finite-dimensional.[4] One motivation for studying continuous-variable quantum computation is to understand what resources are necessary to make quantum computers more powerful than classical ones.[5]

Implementation

One approach to implementing continuous-variable quantum information protocols in the laboratory is through the techniques of quantum optics.[6][7][8] By modeling each mode of the electromagnetic field as a quantum harmonic oscillator with its associated creation and annihilation operators, one defines a canonically conjugate pair of variables for each mode, the so-called "quadratures", which play the role of position and momentum observables. These observables establish a phase space on which Wigner quasiprobability distributions can be defined. Quantum measurements on such a system can be performed using homodyne and heterodyne detectors.

Quantum teleportation of continuous-variable quantum information was achieved by optical methods in 1998.[9][10] (*Science* deemed this experiment one of the "top 10" advances of the year.[11]) In 2013, quantum-optics techniques were used to create a "cluster state", a type of preparation essential to one-way (measurement-based) quantum computation, involving over 10,000 entangled temporal modes, available two at a time.[12] In another implementation, 60 modes were simultaneously entangled in the frequency domain, in the optical frequency comb of an optical parametric oscillator.[13]

Another proposal is to modify the ion-trap quantum computer: instead of storing a single qubit in the internal energy levels of an ion, one could in principle use the position and momentum of the ion as continuous quantum variables.[14]

Applications

Continuous-variable quantum systems can be used for quantum cryptography, and in particular, quantum key distribution.[1] Quantum computing is another potential application, and a variety of approaches have been considered.[1] The first method, proposed by Seth Lloyd and Samuel L. Braunstein in 1999, was in the tradition of the circuit model: quantum logic gates are created by Hamiltonians that, in this case, are quadratic functions of the harmonic-oscillator quadratures.[5] Later, measurement-based quantum

computation was adapted to the setting of infinite-dimensional Hilbert spaces.[15][16] Yet a third model of continuous-variable quantum computation encodes finite-dimensional systems (collections of qubits) into infinite-dimensional ones. This model is due to Daniel Gottesman, Alexei Kitaev and John Preskill.[17]

Classical emulation

In all approaches to quantum computing, it is important to know whether a task under consideration can be carried out efficiently by a classical computer. An algorithm might be described in the language of quantum mechanics, but upon closer analysis, revealed to be implementable using only classical resources. Such an algorithm would not be taking full advantage of the extra possibilities made available by quantum physics. In the theory of quantum computation using finite-dimensional Hilbert spaces, the Gottesman–Knill theorem demonstrates that there exists a set of quantum processes that can be emulated efficiently on a classical computer. Generalizing this theorem to the continuous-variable case, it can be shown that, likewise, a class of continuous-variable quantum computations can be simulated using only classical analog computations. This class includes, in fact, some computational tasks that use quantum entanglement.[18] When the Wigner quasiprobability representations of all the quantities—states, time evolutions *and* measurements—involved in a computation are nonnegative, then they can be interpreted as ordinary probability distributions, indicating that the computation can be modeled as an essentially classical one.[15] This type of construction can be thought of as a continuum generalization of the Spekkens toy model.[19]

Computing continuous functions with discrete quantum systems

Occasionally, and somewhat confusingly, the term "continuous quantum computation" is used to refer to a different area of quantum computing: the study of how to use quantum systems having *finite*-dimensional Hilbert spaces to calculate or approximate the answers to mathematical questions involving continuous functions. A major motivation for investigating the quantum computation of continuous functions is that many scientific problems have mathematical formulations in terms of continuous quantities.[20] A second motivation is to explore and understand the ways in which quantum computers can be more capable or powerful than classical ones. The computational complexity of a problem can be quantified in terms of the minimal computational resources necessary to solve it. In quantum computing, resources include the number of qubits available to a computer and the number of queries that can be made to that computer. The classical complexity of many continuous problems is known. Therefore, when the quantum complexity of these problems is obtained, the question as to whether quantum computers are more powerful than classical can be answered. Furthermore, the degree of the improvement can be quantified. In contrast, the complexity of discrete problems is typically unknown. For example, the classical complexity of integer factorization is unknown.

One example of a scientific problem that is naturally expressed in continuous terms is path integration. The general technique of path integration has numerous applications including quantum mechanics, quantum chemistry, statistical mechanics, and computational finance. Because randomness is present throughout quantum theory, one typically requires that a quantum computational procedure yield the correct answer, not with certainty, but with high probability. For example, one might aim for a procedure that computes the correct answer with probability at least 3/4. One also specifies a degree of uncertainty, typically by setting the maximum acceptable error. Thus, the goal of a quantum computation could be to

compute the numerical result of a path-integration problem to within an error of at most ε with probability 3/4 or more. In this context, it is known that quantum algorithms can outperform their classical counterparts, and the computational complexity of path integration, as measured by the number of times one would expect to have to query a quantum computer to get a good answer, grows as the inverse of ε.[21]

Other continuous problems for which quantum algorithms have been studied include finding matrix eigenvalues,[22] phase estimation,[23] the Sturm–Liouville eigenvalue problem,[24] solving differential equations with the Feynman–Kac formula,[25] initial value problems,[26] function approximation[27] high-dimensional integration.,[28] and quantum cryptography [29]

See also

- Quantum inequalities

References

1. Weedbrook, Christian; Pirandola, Stefano; García-Patrón, Raúl; Cerf, Nicolas J.; Ralph, Timothy C.; Shapiro, Jeffrey H.; Lloyd, Seth (2012-05-01). "Gaussian quantum information". *Reviews of Modern Physics*. **84** (2): 621–669. arXiv:1110.3234 (https://arxiv.org/abs/1110.3234). Bibcode:2012RvMP...84..621W (https://ui.adsabs.harvard.edu/abs/2012RvMP...84..621W). doi:10.1103/RevModPhys.84.621 (https://doi.org/10.1103%2FRevModPhys.84.621). S2CID 119250535 (https://api.semanticscholar.org/CorpusID:119250535).
2. Braunstein, Samuel L.; van Loock, Peter (2005-06-29). "Quantum information with continuous variables". *Reviews of Modern Physics*. **77** (2): 513–577. arXiv:quant-ph/0410100 (https://arxiv.org/abs/quant-ph/0410100). Bibcode:2005RvMP...77..513B (https://ui.adsabs.harvard.edu/abs/2005RvMP...77..513B). doi:10.1103/RevModPhys.77.513 (https://doi.org/10.1103%2FRevModPhys.77.513). S2CID 118990906 (https://api.semanticscholar.org/CorpusID:118990906).
3. Adesso, Gerardo; Ragy, Sammy; Lee, Antony R. (2014-03-12). "Continuous Variable Quantum Information: Gaussian States and Beyond". *Open Systems & Information Dynamics*. **21** (1n02): 1440001. arXiv:1401.4679 (https://arxiv.org/abs/1401.4679). doi:10.1142/S1230161214400010 (https://doi.org/10.1142%2FS1230161214400010). ISSN 1230-1612 (https://search.worldcat.org/issn/1230-1612). S2CID 15318256 (https://api.semanticscholar.org/CorpusID:15318256).
4. Braunstein, S. L.; Pati, A. K. (2012-12-06). *Quantum Information with Continuous Variables*. Springer Science & Business Media. CiteSeerX 10.1.1.762.4959 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.762.4959). doi:10.1007/978-94-015-1258-9 (https://doi.org/10.1007%2F978-94-015-1258-9). ISBN 9789401512589.
5. Lloyd, Seth; Braunstein, Samuel L. (1999-01-01). "Quantum Computation over Continuous Variables". *Physical Review Letters*. **82** (8): 1784–1787. arXiv:quant-ph/9810082 (https://arxiv.org/abs/quant-ph/9810082). Bibcode:1999PhRvL..82.1784L (https://ui.adsabs.harvard.edu/abs/1999PhRvL..82.1784L). doi:10.1103/PhysRevLett.82.1784 (https://doi.org/10.1103%2FPhysRevLett.82.1784). S2CID 119018466 (https://api.semanticscholar.org/CorpusID:119018466).

6. Bartlett, Stephen D.; Sanders, Barry C. (2002-01-01). "Universal continuous-variable quantum computation: Requirement of optical nonlinearity for photon counting". *Physical Review A*. **65** (4): 042304. arXiv:quant-ph/0110039 (https://arxiv.org/abs/quant-ph/0110039). Bibcode:2002PhRvA..65d2304B (https://ui.adsabs.harvard.edu/abs/2002PhRvA..65d2304B). doi:10.1103/PhysRevA.65.042304 (https://doi.org/10.1103%2FPhysRevA.65.042304). S2CID 118896298 (https://api.semanticscholar.org/CorpusID:118896298).
7. Menicucci, Nicolas C.; Flammia, Steven T.; Pfister, Olivier (2008-07-14). "One-way quantum computing in the optical frequency comb". *Physical Review Letters*. **101** (13): 130501. arXiv:0804.4468 (https://arxiv.org/abs/0804.4468). Bibcode:2008PhRvL.101m0501M (https://ui.adsabs.harvard.edu/abs/2008PhRvL.101m0501M). doi:10.1103/PhysRevLett.101.130501 (https://doi.org/10.1103%2FPhysRevLett.101.130501). PMID 18851426 (https://pubmed.ncbi.nlm.nih.gov/18851426). S2CID 1307950 (https://api.semanticscholar.org/CorpusID:1307950).
8. Tasca, D. S.; Gomes, R. M.; Toscano, F.; Souto Ribeiro, P. H.; Walborn, S. P. (2011-01-01). "Continuous-variable quantum computation with spatial degrees of freedom of photons". *Physical Review A*. **83** (5): 052325. arXiv:1106.3049 (https://arxiv.org/abs/1106.3049). Bibcode:2011PhRvA..83e2325T (https://ui.adsabs.harvard.edu/abs/2011PhRvA..83e2325T). doi:10.1103/PhysRevA.83.052325 (https://doi.org/10.1103%2FPhysRevA.83.052325). S2CID 118688635 (https://api.semanticscholar.org/CorpusID:118688635).
9. Furusawa, A.; Sørensen, J. L.; Braunstein, S. L.; Fuchs, C. A.; Kimble, H. J.; Polzik, E. S. (1998-10-23). "Unconditional Quantum Teleportation". *Science*. **282** (5389): 706–709. Bibcode:1998Sci...282..706F (https://ui.adsabs.harvard.edu/abs/1998Sci...282..706F). doi:10.1126/science.282.5389.706 (https://doi.org/10.1126%2Fscience.282.5389.706). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 9784123 (https://pubmed.ncbi.nlm.nih.gov/9784123).
10. Braunstein, Samuel L.; Fuchs, Christopher A.; Kimble, H. J. (2000-02-01). "Criteria for continuous-variable quantum teleportation". *Journal of Modern Optics*. **47** (2–3): 267–278. arXiv:quant-ph/9910030 (https://arxiv.org/abs/quant-ph/9910030). Bibcode:2000JMOp...47..267B (https://ui.adsabs.harvard.edu/abs/2000JMOp...47..267B). doi:10.1080/09500340008244041 (https://doi.org/10.1080%2F09500340008244041). ISSN 0950-0340 (https://search.worldcat.org/issn/0950-0340). S2CID 16713029 (https://api.semanticscholar.org/CorpusID:16713029).
11. "The Runners-Up: The News and Editorial Staffs". *Science*. **282** (5397): 2157–2161. 1998-12-18. Bibcode:1998Sci...282.2157. (https://ui.adsabs.harvard.edu/abs/1998Sci...282.2157.). doi:10.1126/science.282.5397.2157 (https://doi.org/10.1126%2Fscience.282.5397.2157). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). S2CID 220101560 (https://api.semanticscholar.org/CorpusID:220101560).
12. Yokoyama, Shota; Ukai, Ryuji; Armstrong, Seiji C.; Sornphiphatphong, Chanond; Kaji, Toshiyuki; Suzuki, Shigenari; Yoshikawa, Jun-ichi; Yonezawa, Hidehiro; Menicucci, Nicolas C. (2013). "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain". *Nature Photonics*. **7** (12): 982–986. arXiv:1306.3366 (https://arxiv.org/abs/1306.3366). Bibcode:2013NaPho...7..982Y (https://ui.adsabs.harvard.edu/abs/2013NaPho...7..982Y). doi:10.1038/nphoton.2013.287 (https://doi.org/10.1038%2Fnphoton.2013.287). S2CID 53575929 (https://api.semanticscholar.org/CorpusID:53575929).
13. Chen, Moran; Menicucci, Nicolas C.; Pfister, Olivier (2014-03-28). "Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb". *Physical Review Letters*. **112** (12): 120505. arXiv:1311.2957 (https://arxiv.org/abs/1311.2957). Bibcode:2014PhRvL.112l0505C (https://ui.adsabs.harvard.edu/abs/2014PhRvL.112l0505C). doi:10.1103/PhysRevLett.112.120505 (https://doi.org/10.1103%2FPhysRevLett.112.120505). PMID 24724640 (https://pubmed.ncbi.nlm.nih.gov/24724640). S2CID 18093254 (https://api.semanticscholar.org/CorpusID:18093254).

14. Ortiz-Gutiérrez, Luis; Gabrielly, Bruna; Muñoz, Luis F.; Pereira, Kainã T.; Filgueiras, Jefferson G.; Villar, Alessandro S. (2017-08-15). "Continuous variables quantum computation over the vibrational modes of a single trapped ion". *Optics Communications*. **397**: 166–174. arXiv:1603.00065 (https://arxiv.org/abs/1603.00065). Bibcode:2017OptCo.397..166O (https://ui.adsabs.harvard.edu/abs/2017OptCo.397..166O). doi:10.1016/j.optcom.2017.04.011 (https://doi.org/10.1016%2Fj.optcom.2017.04.011). S2CID 118617424 (https://api.semanticscholar.org/CorpusID:118617424).
15. Menicucci, Nicolas C.; van Loock, Peter; Gu, Mile; Weedbrook, Christian; Ralph, Timothy C.; Nielsen, Michael A. (2006-09-13). "Universal Quantum Computation with Continuous-Variable Cluster States". *Physical Review Letters*. **97** (11): 110501. arXiv:quant-ph/0605198 (https://arxiv.org/abs/quant-ph/0605198). Bibcode:2006PhRvL..97k0501M (https://ui.adsabs.harvard.edu/abs/2006PhRvL..97k0501M). doi:10.1103/PhysRevLett.97.110501 (https://doi.org/10.1103%2FPhysRevLett.97.110501). PMID 17025869 (https://pubmed.ncbi.nlm.nih.gov/17025869). S2CID 14715751 (https://api.semanticscholar.org/CorpusID:14715751).
16. Zhang, Jing; Braunstein, Samuel L. (2006-03-16). "Continuous-variable Gaussian analog of cluster states". *Physical Review A*. **73** (3): 032318. arXiv:quant-ph/0501112 (https://arxiv.org/abs/quant-ph/0501112). Bibcode:2006PhRvA..73c2318Z (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73c2318Z). doi:10.1103/PhysRevA.73.032318 (https://doi.org/10.1103%2FPhysRevA.73.032318). S2CID 119511825 (https://api.semanticscholar.org/CorpusID:119511825).
17. Gottesman, Daniel; Kitaev, Alexei; Preskill, John (2001-06-11). "Encoding a qubit in an oscillator". *Physical Review A*. **64** (1): 012310. arXiv:quant-ph/0008040 (https://arxiv.org/abs/quant-ph/0008040). Bibcode:2001PhRvA..64a2310G (https://ui.adsabs.harvard.edu/abs/2001PhRvA..64a2310G). doi:10.1103/PhysRevA.64.012310 (https://doi.org/10.1103%2FPhysRevA.64.012310). S2CID 18995200 (https://api.semanticscholar.org/CorpusID:18995200).
18. Bartlett, Stephen D.; Sanders, Barry C.; Braunstein, Samuel L.; Nemoto, Kae (2002-02-14). "Efficient Classical Simulation of Continuous Variable Quantum Information Processes". *Physical Review Letters*. **88** (9): 097904. arXiv:quant-ph/0109047 (https://arxiv.org/abs/quant-ph/0109047). Bibcode:2002PhRvL..88i7904B (https://ui.adsabs.harvard.edu/abs/2002PhRvL..88i7904B). doi:10.1103/PhysRevLett.88.097904 (https://doi.org/10.1103%2FPhysRevLett.88.097904). PMID 11864057 (https://pubmed.ncbi.nlm.nih.gov/11864057). S2CID 2161585 (https://api.semanticscholar.org/CorpusID:2161585).
19. Bartlett, Stephen D.; Rudolph, Terry; Spekkens, Robert W. (2012-07-10). "Reconstruction of Gaussian quantum mechanics from Liouville mechanics with an epistemic restriction". *Physical Review A*. **86** (1): 012103. arXiv:1111.5057 (https://arxiv.org/abs/1111.5057). Bibcode:2012PhRvA..86a2103B (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86a2103B). doi:10.1103/PhysRevA.86.012103 (https://doi.org/10.1103%2FPhysRevA.86.012103). S2CID 119235025 (https://api.semanticscholar.org/CorpusID:119235025).
20. Papageorgiou, A. "Continuous Quantum Computation: Project Description" (http://quantum.cs.columbia.edu/html/project.html). *quantum.cs.columbia.edu*. Retrieved 2017-05-15.
21. Traub, J. F.; Woźniakowski, H. (2002-10-01). "Path Integration on a Quantum Computer". *Quantum Information Processing*. **1** (5): 365–388. arXiv:quant-ph/0109113 (https://arxiv.org/abs/quant-ph/0109113). doi:10.1023/A:1023417813916 (https://doi.org/10.1023%2FA%3A1023417813916). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 5821196 (https://api.semanticscholar.org/CorpusID:5821196).
22. Jaksch, Peter; Papageorgiou, Anargyros (2003-12-19). "Eigenvector Approximation Leading to Exponential Speedup of Quantum Eigenvalue Calculation". *Physical Review Letters*. **91** (25): 257902. arXiv:quant-ph/0308016 (https://arxiv.org/abs/quant-ph/0308016). Bibcode:2003PhRvL..91y7902J (https://ui.adsabs.harvard.edu/abs/2003PhRvL..91y7902J). doi:10.1103/PhysRevLett.91.257902 (https://doi.org/10.1103%2FPhysRevLett.91.257902). PMID 14754158 (https://pubmed.ncbi.nlm.nih.gov/14754158). S2CID 1855075 (https://api.semanticscholar.org/CorpusID:1855075).

23. Bessen, Arvid J. (2005-04-08). "Lower bound for quantum phase estimation". *Physical Review A*. **71** (4): 042313. arXiv:quant-ph/0412008 (https://arxiv.org/abs/quant-ph/0412008). Bibcode:2005PhRvA..71d2313B (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71d2313B). doi:10.1103/PhysRevA.71.042313 (https://doi.org/10.1103%2FPhysRevA.71.042313). S2CID 118887469 (https://api.semanticscholar.org/CorpusID:118887469).
24. Papageorgiou, A.; Woźniakowski, H (2005). "Classical and Quantum Complexity of the Sturm–Liouville Eigenvalue Problem". *Quantum Information Processing*. **4** (2): 87–127. arXiv:quant-ph/0502054 (https://arxiv.org/abs/quant-ph/0502054). Bibcode:2005quant.ph..2054P (https://ui.adsabs.harvard.edu/abs/2005quant.ph..2054P). doi:10.1007/s11128-005-4481-x (https://doi.org/10.1007%2Fs11128-005-4481-x). S2CID 11089349 (https://api.semanticscholar.org/CorpusID:11089349).
Papageorgiou, A.; Woźniakowski, H. (2007-04-01). "The Sturm-Liouville Eigenvalue Problem and NP-Complete Problems in the Quantum Setting with Queries". *Quantum Information Processing*. **6** (2): 101–120. arXiv:quant-ph/0504191 (https://arxiv.org/abs/quant-ph/0504191). doi:10.1007/s11128-006-0043-0 (https://doi.org/10.1007%2Fs11128-006-0043-0). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 7604869 (https://api.semanticscholar.org/CorpusID:7604869).
25. Kwas, Marek (2004-10-18). "Complexity of multivariate Feynman-Kac path integration in randomized and quantum settings". arXiv:quant-ph/0410134 (https://arxiv.org/abs/quant-ph/0410134).
26. Kacewicz, Bolesław (2004). "Randomized and quantum algorithms yield a speed-up for initial-value problems". *Journal of Complexity*. **20** (6): 821–834. arXiv:quant-ph/0311148 (https://arxiv.org/abs/quant-ph/0311148). doi:10.1016/j.jco.2004.05.002 (https://doi.org/10.1016%2Fj.jco.2004.05.002). S2CID 9949704 (https://api.semanticscholar.org/CorpusID:9949704).
Szczesny, Marek (2006-12-12). "Randomized and Quantum Solution of Initial-Value Problems for Ordinary Differential Equations of Order k". arXiv:quant-ph/0612085 (https://arxiv.org/abs/quant-ph/0612085).
Kacewicz, Bolesław (2005). "Improved bounds on the randomized and quantum complexity of initial-value problems". *Journal of Complexity*. **21** (5): 740–756. arXiv:quant-ph/0405018 (https://arxiv.org/abs/quant-ph/0405018). doi:10.1016/j.jco.2005.05.003 (https://doi.org/10.1016%2Fj.jco.2005.05.003). S2CID 5934254 (https://api.semanticscholar.org/CorpusID:5934254).
27. Novak, Erich; Sloan, Ian H.; Woźniakowski, Henryk (2004-04-01). "Tractability of Approximation for Weighted Korobov Spaces on Classical and Quantum Computers". *Foundations of Computational Mathematics*. **4** (2): 121–156. arXiv:quant-ph/0206023 (https://arxiv.org/abs/quant-ph/0206023). doi:10.1007/s10208-002-0074-6 (https://doi.org/10.1007%2Fs10208-002-0074-6). ISSN 1615-3375 (https://search.worldcat.org/issn/1615-3375). S2CID 10519614 (https://api.semanticscholar.org/CorpusID:10519614).
Heinrich, Stefan (2004). "Quantum approximation I. Embeddings of finite-dimensional Lp spaces". *Journal of Complexity*. **20** (1): 5–26. arXiv:quant-ph/0305030 (https://arxiv.org/abs/quant-ph/0305030). doi:10.1016/j.jco.2003.08.002 (https://doi.org/10.1016%2Fj.jco.2003.08.002). S2CID 6044488 (https://api.semanticscholar.org/CorpusID:6044488).
Heinrich, Stefan (2004). "Quantum approximation II. Sobolev embeddings". *Journal of Complexity*. **20** (1): 27–45. arXiv:quant-ph/0305031 (https://arxiv.org/abs/quant-ph/0305031). doi:10.1016/j.jco.2003.08.003 (https://doi.org/10.1016%2Fj.jco.2003.08.003). S2CID 6061625 (https://api.semanticscholar.org/CorpusID:6061625).

28. Heinrich, Stefan (2002). "Quantum Summation with an Application to Integration". *Journal of Complexity*. **18** (1): 1–50. arXiv:quant-ph/0105116 (https://arxiv.org/abs/quant-ph/0105116). doi:10.1006/jcom.2001.0629 (https://doi.org/10.1006%2Fjcom.2001.0629). S2CID 14365504 (https://api.semanticscholar.org/CorpusID:14365504).
Heinrich, Stefan (2003-02-01). "Quantum integration in Sobolev classes". *Journal of Complexity*. **19** (1): 19–42. arXiv:quant-ph/0112153 (https://arxiv.org/abs/quant-ph/0112153). doi:10.1016/S0885-064X(02)00008-0 (https://doi.org/10.1016%2FS0885-064X%2802%2900008-0). S2CID 5471897 (https://api.semanticscholar.org/CorpusID:5471897).
Novak, Erich (2001). "Quantum Complexity of Integration". *Journal of Complexity*. **17** (1): 2–16. arXiv:quant-ph/0008124 (https://arxiv.org/abs/quant-ph/0008124). doi:10.1006/jcom.2000.0566 (https://doi.org/10.1006%2Fjcom.2000.0566). S2CID 2271590 (https://api.semanticscholar.org/CorpusID:2271590).
29. Mu, Yi (1996). "Shared cryptographic bits via quantized quadrature phase amplitudes of light". *Journal of Optics Communication*. **123** (1–3): 334–352. Bibcode:1996OptCo.123..344M (https://ui.adsabs.harvard.edu/abs/1996OptCo.123..344M). doi:10.1016/0030-4018(95)00688-5 (https://doi.org/10.1016%2F0030-4018%2895%2900688-5). S2CID 18374270 (https://api.semanticscholar.org/CorpusID:18374270).

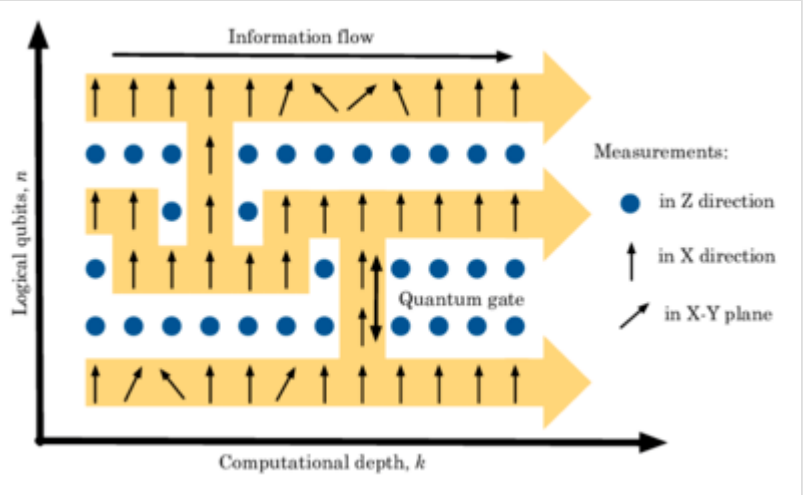
Retrieved from "https://en.wikipedia.org/w/index.php?title=Continuous-variable_quantum_information&oldid=1223538918"

WIKIPEDIA
The Free Encyclopedia

One-way quantum computer

The **one-way quantum computer**, also known as **measurement-based quantum computer** (**MBQC**), is a method of quantum computing that first prepares an entangled *resource state*, usually a cluster state or graph state, then performs single qubit measurements on it. It is "one-way" because the resource state is destroyed by the measurements.

The outcome of each individual measurement is random, but they are related in such a way that the computation always succeeds. In general, the choices of basis for later measurements need to depend on the results of earlier measurements, and hence the measurements cannot all be performed at the same time.



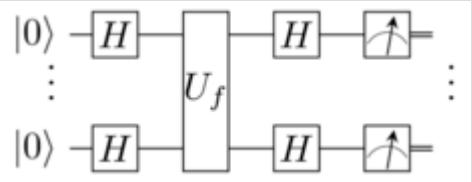
The measurement-based techniques consist of entangling a cluster of qubits and performing a set of measurements. Thanks to the correlation between the entangled qubits, the flow of information (from left to right) is carried on by the measurements on the physical qubits in the cluster.

The hardware implementation of MBQC mainly relies on photonic devices,[1] due to the difficulty of entangling photons without measurements, and the relative simplicity of creating and measuring them. However, MBQC is also possible with matter-based qubits.[2] The process of entanglement and measurement can be described with the help of graph tools and group theory, in particular by the elements from the stabilizer group.

Definition

The purpose of quantum computing focuses on building an information theory with the features of quantum mechanics: instead of encoding a binary unit of information (bit), which can be switched to 1 or 0, a quantum binary unit of information (qubit) can simultaneously turn to be 0 and 1 at the same time, thanks to the phenomenon called superposition.[3][4][5] Another key feature for quantum computing relies on the entanglement between the qubits.[6][7][8]

In the quantum logic gate model, a set of qubits, called register, is prepared at the beginning of the computation, then a set of logic operations over the qubits, carried by unitary operators, is implemented.[9][10] A quantum circuit is formed by a register of qubits on which unitary transformations are applied over the qubits. In the measurement-based quantum computation, instead of implementing a logic operation via unitary transformations, the same operation is executed by entangling a number k of input qubits with a cluster of a ancillary qubits, forming an overall source state of $a + k = n$ qubits, and



A quantum circuit implementing the Bernstein-Vazirani algorithm: H and U_f represent the logic gates (unitary operators) which act on the register of qubits. In the *MBQC* frame, the logic gates are performed by entangling the qubits and measuring the auxiliary ones.

then measuring a number m of them.[11][12] The remaining $k = n - a$ output qubits will be affected by the measurements because of the entanglement with the measured qubits. The one-way computer has been proved to be a universal quantum computer, which means it can reproduce any unitary operation over an arbitrary number of qubits.[9][13][14][15]

General procedure

The standard process of measurement-based quantum computing consists of three steps:[16][17] entangle the qubits, measure the ancillae (auxiliary qubits) and correct the outputs. In the first step, the qubits are entangled in order to prepare the source state. In the second step, the ancillae are measured, affecting the state of the output qubits. However, the measurement outputs are non-deterministic result, due to undetermined nature of quantum mechanics:[17] in order to carry on the computation in a deterministic way, some correction operators, called byproducts, are introduced.

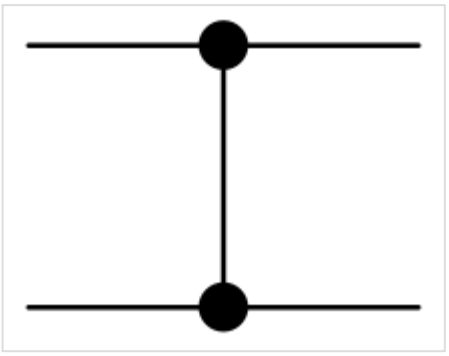
Preparing the source state

At the beginning of the computation, the qubits can be distinguished into two categories: the input and the ancillary qubits. The inputs represent the qubits set in a generic $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ state, on which some unitary transformations are to be acted. In order to prepare the source state, all the ancillary qubits must be prepared in the $|+\rangle$ state:[11][18]

$$|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}},$$

where $|0\rangle$ and $|1\rangle$ are the quantum encoding for the classical 0 and 1 bits:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$



The *CZ* operation in the circuit diagrams.

A register with n qubits will be therefore set as $|+\rangle^{\otimes n}$. Thereafter, the entanglement between two qubits can be performed by applying a CZ gate operation.[19] The matrix representation of such two-qubits operator is given by

$$CZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}.$$

The action of a CZ gate over two qubits can be described by the following system:

$$\begin{cases} CZ|0+\rangle = |0+\rangle \\ CZ|0-\rangle = |0-\rangle \\ CZ|1+\rangle = |1-\rangle \\ CZ|1-\rangle = |1+\rangle \end{cases}$$

When applying a CZ gate over two ancillae in the $|+\rangle$ state, the overall state

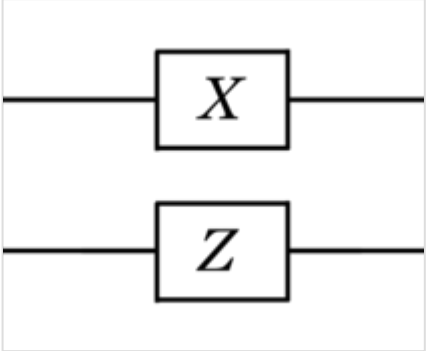
$$CZ|++\rangle = \frac{|0+\rangle + |1-\rangle}{\sqrt{2}}$$

turns to be an entangled pair of qubits. When entangling two ancillae, no importance is given about which is the control qubit and which one the target, as far as the outcome turns to be the same. Similarly, as the CZ gates are represented in a diagonal form, they all commute each other, and no importance is given about which qubits to entangle first. Photons are the most common source to prepare entangled physical qubits.[20][21][22]

Measuring the qubits

The process of measurement over a single-particle state can be described by projecting the state on the eigenvector of an observable. Consider an observable O with two possible eigenvectors, say $|o_1\rangle$ and $|o_2\rangle$, and suppose to deal with a multi-particle quantum system $|\Psi\rangle$. Measuring the i-th qubit by the O observable means to project the $|\Psi\rangle$ state over the eigenvectors of O:[18]

$$|\Psi'\rangle = |o_i\rangle\langle o_i|\Psi\rangle.$$



Implementation of *X* and *Z* gates over two qubits in the circuit diagrams.

The actual state of the i-th qubit is now $|o_i\rangle$, which can turn to be $|o_1\rangle$ or $|o_2\rangle$, depending on the outcome from the measurement (which is probabilistic in quantum mechanics). The measurement projection can be performed over the eigenstates of the $M(\theta) = \cos(\theta)X + \sin(\theta)Y$ observable:

$$M(\theta) = \cos(\theta)\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \sin(\theta)\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & e^{-i\theta} \\ e^{i\theta} & 0 \end{bmatrix},$$

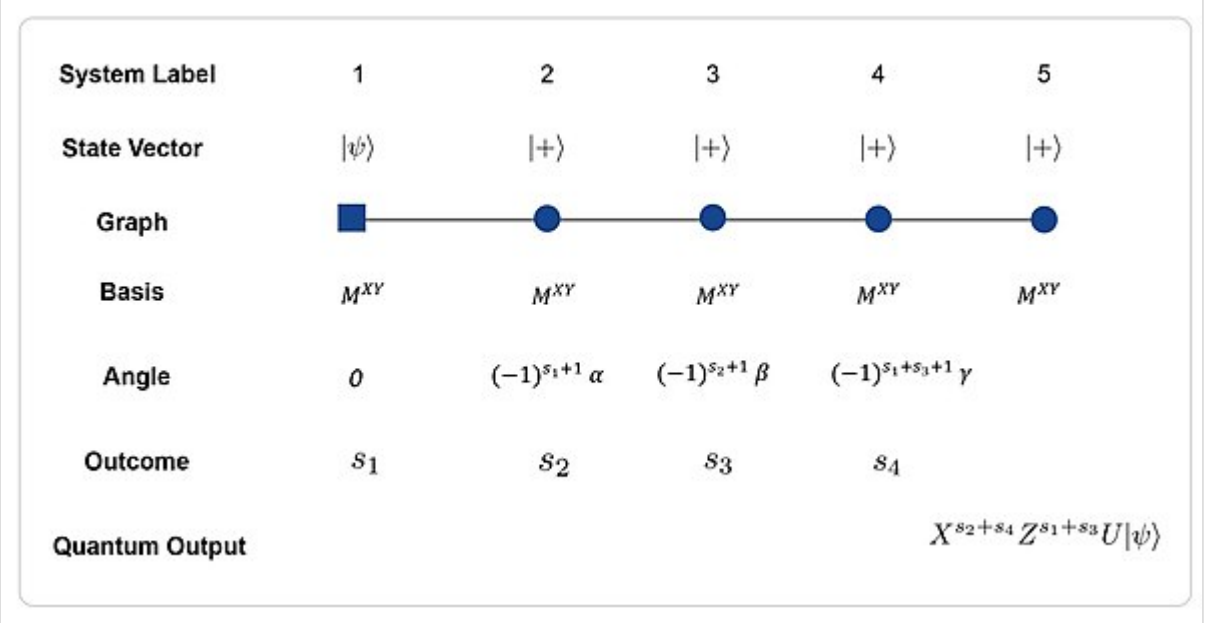
where X and Y belong to the Pauli matrices. The eigenvectors of $M(\theta)$ are $|\theta_\pm\rangle = |0\rangle \pm e^{i\theta}|1\rangle$. Measuring a qubit on the X-Y plane, i.e. by the $M(\theta)$ observable, means to project it over $|\theta_+\rangle$ or $|\theta_-\rangle$. In the one-way quantum computing, once a qubit has been measured, there is no way to recycle it in the flow of computation. Therefore, instead of using the $|o_i\rangle\langle o_i|$ notation, it is common to find $\langle o_i|$ to indicate a projective measurement over the i-th qubit.

Correcting the output

After all the measurements have been performed, the system has been reduced to a smaller number of qubits, which form the output state of the system. Due to the probabilistic outcome of measurements, the system is not set in a deterministic way: after a measurement on the X-Y plane, the output may change

whether the outcome had been $|\theta_+\rangle$ or $|\theta_-\rangle$. In order to perform a deterministic computation, some corrections must be introduced. The correction operators, or byproduct operators, are applied to the output qubits after all the measurements have been performed.[18][23] The byproduct operators which can be implemented are X and Z.[24] Depending on the outcome of the measurement, a byproduct operator can be applied or not to the output state: a X correction over the j-th qubit, depending on the outcome of the measurement performed over the i-th qubit via the $M(\theta)$ observable, can be described as $X_j^{s_i}$, where s_i is set to be 0 if the outcome of measurement was $|\theta_+\rangle$, otherwise is 1 if it was $|\theta_-\rangle$. In the first case, no correction will occur, in the latter one a X operator will be implemented on the j-th qubit. Eventually, even though the outcome of a measurement is not deterministic in quantum mechanics, the results from measurements can be used in order to perform corrections, and carry on a deterministic computation.

CME pattern



The Euler rotation (with respect to the XZX basis) in the MBQC computation. The lines describe the entanglement between the qubits. The first qubit corresponds to the input state $|\psi\rangle$, the fifth one to the output state. The qubits from 2 to 4 are the ancillae. All the states, except for the input, are prepared in the $|+\rangle$ state. All the qubits, except for the output, are measured by the M observable with a specific angle. After the measurements have been carried on, implementing the U unitary, the X and Z corrections are performed with respect to the s_i outcomes.

The operations of entanglement, measurement and correction can be performed in order to implement unitary gates. Such operations can be performed time by time for any logic gate in the circuit, or rather in a pattern which allocates all the entanglement operations at the beginning, the measurements in the middle and the corrections at the end of the circuit. Such pattern of computation is referred to as *CME* standard pattern.[16][17] In the *CME* formalism, the operation of entanglement between the i and j qubits is referred to as E_{ij}. The measurement on the i qubit, in the X-Y plane, with respect to a θ angle, is defined as M_i^θ. At last, the X byproduct over a i qubit, with respect to the measurement over a j qubit, is described as $X_i^{s_j}$, where s_j is set to 0 if the outcome is the $|\theta_+\rangle$ state, 1 when the outcome is $|\theta_-\rangle$. The same notation holds for the Z byproducts.

When performing a computation following the *CME* pattern, it may happen that two measurements $M_i^{\theta_1}$ and $M_j^{\theta_2}$ on the X-Y plane depend one on the outcome from the other. For example, the sign in front of the angle of measurement on the j-th qubit can be flipped with respect to the measurement over the i-th qubit: in such case, the notation will be written as $[M_j^{\theta_2}]^{s_i} M_i^{\theta_1}$, and therefore the two operations of measurement do commute each other no more. If s_i is set to 0, no flip on the θ_2 sign will occur, otherwise (when $s_i = 1$) the θ_2 angle will be flipped to $-\theta_2$. The notation $[M_j^{\theta_2}]^{s_i}$ can therefore be rewritten as $M_j^{(-)^{s_i}\theta_2}$.

An example: Euler rotations

As an illustrative example, consider the Euler rotation in the XZX basis: such operation, in the gate model of quantum computation, is described as[25]

$$e^{i\gamma} R_X(\phi) R_Z(\theta) R_X(\lambda),$$

where ϕ, θ, λ are the angles for the rotation, while γ defines a global phase which is irrelevant for the computation. To perform such operation in the one-way computing frame, it is possible to implement the following *CME* pattern:[23][26]

$$Z_5^{s_1+s_3} X_5^{s_2+s_4} [M_4^{-\phi}]^{s_1+s_3} [M_3^{-\theta}]^{s_2} [M_2^{-\lambda}]^{s_1} M_1^0 E_{4,5} E_{3,4} E_{2,3} E_{1,2},$$

where the input state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is the qubit 1, all the other qubits are auxiliary ancillae and therefore have to be prepared in the $|+\rangle$ state. In the first step, the input state $|\psi\rangle$ must be entangled with the second qubits; in turn, the second qubit must be entangled with the third one and so on. The entangling operations E_{ij} between the qubits can be performed by the CZ gates.

In the second place, the first and the second qubits must be measured by the $M(\theta)$ observable, which means they must be projected onto the eigenstates $|\theta\rangle$ of such observable. When the θ is zero, the $|\theta_\pm\rangle$ states reduce to $|\pm\rangle$ ones, i.e. the eigenvectors for the X Pauli operator. The first measurement M_1^0 is performed on the qubit 1 with a $\theta = 0$ angle, which means it has to be projected onto the $\langle\pm|$ states. The second measurement $[M_2^{-\lambda}]^{s_1}$ is performed with respect to the $-\lambda$ angle, i.e. the second qubit has to be projected on the $\langle 0| \pm e^{i\lambda}\langle 1|$ state. However, if the outcome from the previous measurement has been $\langle -|$, the sign of the λ angle has to be flipped, and the second qubit will be projected to the $\langle 0| + e^{-i\lambda}\langle 1|$ state; if the outcome from the first measurement has been $\langle +|$, no flip needs to be performed. The same operations have to be repeated for the third $[M_3^{\theta}]^{s_2}$ and the fourth $[M_4^{\phi}]^{s_1+s_3}$ measurements, according to the respective angles and sign flips. The sign over the ϕ angle is set to be $(-)^{s_1+s_3}$. Eventually the fifth qubit (the only one not to be measured) figures out to be the output state.

At last, the corrections $Z_5^{s_1+s_3} X_5^{s_2+s_4}$ over the output state have to be performed via the byproduct operators. For instance, if the measurements over the second and the fourth qubits turned to be $\langle\phi_+|$ and $\langle\lambda_+|$, no correction will be conducted by the X_5 operator, as $s_2 = s_4 = 0$. The same result holds for a $\langle\phi_-|\ \langle\lambda_-|$ outcome, as $s_2 = s_4 = 1$ and thus the squared Pauli operator X^2 returns the identity.

As seen in such example, in the measurement-based computation model, the physical input qubit (the first one) and output qubit (the third one) may differ each other.

Equivalence between quantum circuit model and MBQC

The one-way quantum computer allows the implementation of a circuit of unitary transformations through the operations of entanglement and measurement. At the same time, any quantum circuit can be in turn converted into a *CME* pattern: a technique to translate quantum circuits into a *MBQC* pattern of measurements has been formulated by V. Danos et al.[16][17][27]

Such conversion can be carried on by using a universal set of logic gates composed by the CZ and the $J(\theta)$ operators: therefore, any circuit can be decomposed into a set of CZ and the $J(\theta)$ gates. The $J(\theta)$ single-qubit operator is defined as follows:

$$J(\theta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\theta} \\ 1 & -e^{i\theta} \end{pmatrix}.$$

The $J(\theta)$ can be converted into a *CME* pattern as follows, with qubit 1 being the input and qubit 2 being the output:

$$J(\theta) = X_2^{s_1} M_1^{-\theta} E_{1,2}$$

which means, to implement a $J(\theta)$ operator, the input qubits $|\psi\rangle$ must be entangled with an ancilla qubit $|+\rangle$, therefore the input must be measured on the X-Y plane, thereafter the output qubit is corrected by the X_2 byproduct. Once every $J(\theta)$ gate has been decomposed into the *CME* pattern, the operations in the overall computation will consist of E_{ij} entanglements, $M_i^{-\theta_i}$ measurements and X_j corrections. In order to lead the whole flow of computation to a *CME* pattern, some rules are provided.

Standardization

In order to move all the E_{ij} entanglements at the beginning of the process, some rules of commutation must be pointed out:

$$\begin{aligned} E_{ij} Z_i^s &= Z_i^s E_{ij} \\ E_{ij} X_i^s &= X_i^s Z_j^s E_{ij} \\ E_{ij} A_k &= A_k E_{ij}. \end{aligned}$$

The entanglement operator E_{ij} commutes with the Z Pauli operators and with any other operator A_k acting on a qubit $k \neq i, j$, but not with the X Pauli operators acting on the i-th or j-th qubits.

Pauli simplification

The measurement operations M_i^θ commute with the corrections in the following manner:

$$\begin{aligned} M_i^\theta X_i^s &= [M_i^\theta]^s \\ M_i^\theta Z_i^t &= S_i^t M_i^\theta, \end{aligned}$$

where $[M_i^\theta]^s = M_i^{(-)^s\theta}$. Such operation means that, when shifting the X corrections at the end of the pattern, some dependencies between the measurements may occur. The S_i^t operator is called signal shifting, whose action will be explained in the next paragraph. For particular θ angles, some simplifications, called Pauli simplifications, can be introduced:

$$M_i^0 X_i^s = M_i^0$$
$$M_i^{\pi/2} X_i^s = M_i^{\pi/2} Z_i^s.$$

Signal shifting

The action of the signal shifting operator S_i^t can be explained through its rules of commutation:

$$X_i^s S_i^t = S_i^t X_i^{s[(s_i+t)/s_i]}$$
$$Z_i^s S_i^t = S_i^t Z_i^{s[(s_i+t)/s_i]}.$$

The $s[(t+s_i)/s_i]$ operation has to be explained: suppose to have a sequence of signals s, consisting of $s_1 + s_2 + \ldots + s_i + \ldots$, the operation $s[(t+s_i)/s_i]$ means to substitute s_i with $s_i + t$ in the sequence s, which becomes $s_1 + s_2 + \ldots + s_i + t + \ldots$. If no s_i appears in the s sequence, no substitution will occur. To perform a correct *CME* pattern, every signal shifting operator S_i^t must be translated at the end of the pattern.

Stabilizer formalism

When preparing the source state of entangled qubits, a graph representation can be given by the stabilizer group. The stabilizer group $\mathcal{S}_n$ is an abelian subgroup from the Pauli group $\mathcal{P}_n$, which one can be described by its generators $\{\pm 1, \pm i\} \times \{I, X, Y, Z\}^{\otimes n}$.[28][29] A stabilizer state is a n-qubit state $|\Psi\rangle$ which is a unique eigenstate for the generators S_i of the $\mathcal{S}_n$ stabilizer group:[19]

$$S_i|\Psi\rangle = |\Psi\rangle.$$

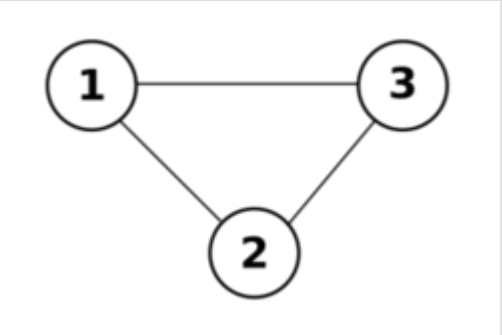
Of course, $S_i \in \mathcal{S}_n \; \forall i$.

It is therefore possible to define a n qubit graph state $|G\rangle$ as a quantum state associated with a graph, i.e. a set $G = (V, E)$ whose vertices V correspond to the qubits, while the edges E represent the entanglements between the qubits themselves. The vertices can be labelled by a i index, while the edges, linking the i-th vertex to the j-th one, by two-indices labels, such as (i, j).[30] In the stabilizer formalism, such graph structure can be encoded by the K_i generators of $\mathcal{S}_n$, defined as[15][31][32]

$$K_i = X_i \prod_{j \in (i,j)} Z_j,$$

where $j \in (i, j)$ stands for all the j qubits neighboring with the i-th one, i.e. the j vertices linked by a (i, j) edge with the i vertex. Each K_i generator commute with all the others. A graph composed by n vertices can be described by n generators from the stabilizer group:

$$\langle K_1, K_2, \ldots, K_n \rangle.$$



A math graph defined by three vertices and three edges. Each vertex is connected with the other ones by an edge. In the MBQC frame, the vertices $1, 2, 3$ represent the qubits, while the links between them the entanglements. In the stabilizer formalism, such graph is represented by the $\langle X_1 Z_2 Z_3, Z_1 X_2 Z_3, Z_1 Z_2 X_3 \rangle$ generators, which all of them commute each other with.

While the number of X_i is fixed for each K_i generator, the number of Z_j may differ, with respect to the connections implemented by the edges in the graph.

The Clifford group

The Clifford group $\mathcal{C}_n$ is composed by elements which leave invariant the elements from the Pauli's group $\mathcal{P}_n$:[19][29][33]

$$\mathcal{C}_n = \{U \in SU(2^n) \mid USU^\dagger \in \mathcal{P}_n, S \in \mathcal{P}_n\}.$$

The Clifford group requires three generators, which can be chosen as the Hadamard gate H and the phase rotation S for the single-qubit gates, and another two-qubits gate from the $CNOT$ (controlled NOT gate) or the CZ (controlled phase gate):

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Consider a state $|G\rangle$ which is stabilized by a set of stabilizers S_i. Acting via an element U from the Clifford group on such state, the following equalities hold:[29][34]

$$U|G\rangle = US_i|G\rangle = US_iU^\dagger U|G\rangle = S_i'U|G\rangle.$$

Therefore, the U operations map the $|G\rangle$ state to $U|G\rangle$ and its S_i stabilizers to $US_iU^\dagger$. Such operation may give rise to different representations for the K_i generators of the stabilizer group.

The Gottesman–Knill theorem states that, given a set of logic gates from the Clifford group, followed by Z measurements, such computation can be efficiently simulated on a classical computer in the strong sense, i.e. a computation which elaborates in a polynomial-time the probability $P(x)$ for a given output x from the circuit.[19][29][35][36][37]

Hardware and applications

Topological cluster state quantum computer

Measurement-based computation on a periodic 3D lattice cluster state can be used to implement topological quantum error correction.[38] Topological cluster state computation is closely related to Kitaev's toric code, as the 3D topological cluster state can be constructed and measured over time by a repeated sequence of gates on a 2D array.[39]

Implementations

One-way quantum computation has been demonstrated by running the 2 qubit Grover's algorithm on a 2x2 cluster state of photons.[40][41] A linear optics quantum computer based on one-way computation has been proposed.[42]

Cluster states have also been created in optical lattices,[43] but were not used for computation as the atom qubits were too close together to measure individually.

AKLT state as a resource

It has been shown that the (spin $\frac{3}{2}$) AKLT state on a 2D honeycomb lattice can be used as a resource for MBQC.[44][45] More recently it has been shown that a spin-mixture AKLT state can be used as a resource.[46]

See also

- Quantum gate teleportation
- Continuous-variable quantum information
- Quantum algorithm
- Quantum logic gate
- Linear optical quantum computing
- Quantum optics
- Quantum error correction
- Quantum Turing machine
- Adiabatic quantum computation

References

1. Fowler, Austin G.; Goyal, Kovid (2009-02-25). "Topological cluster state quantum computing" (https://dl.acm.org/doi/10.5555/2011804.2011805). *Quantum Information & Computation*. **9** (9&10): 721–738. arXiv:0805.3202 (https://arxiv.org/abs/0805.3202). doi:10.26421/QIC9.9-10-1 (https://doi.org/10.26421%2FQIC9.9-10-1). S2CID 6652655 (https://api.semanticscholar.org/CorpusID:6652655).
2. Raussendorf, R; Harrington, J; Goyal, K (2007-06-29). "Topological fault-tolerance in cluster state quantum computation" (https://iopscience.iop.org/article/10.1088/1367-2630/9/6/199). *New Journal of Physics*. **9** (6): 199. arXiv:quant-ph/0703143 (https://arxiv.org/abs/quant-ph/0703143). Bibcode:2007NJPh....9..199R (https://ui.adsabs.harvard.edu/abs/2007NJPh....9..199R). doi:10.1088/1367-2630/9/6/199 (https://doi.org/10.1088%2F1367-2630%2F9%2F6%2F199). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 13811487 (https://api.semanticscholar.org/CorpusID:13811487).

3. S. S. Li; G. L. Long; F. S. Bai; S. L. Feng; H. Z. Zheng (2001). "Quantum computing" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC59812). *Proceedings of the National Academy of Sciences*. **98** (21): 11847–11848. Bibcode:2001PNAS...9811847L (https://ui.adsabs.harvard.edu/abs/2001PNAS...9811847L). doi:10.1073/pnas.191373698 (https://doi.org/10.1073%2Fpnas.191373698). PMC 59812 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC59812). PMID 11562459 (https://pubmed.ncbi.nlm.nih.gov/11562459).
4. E. Grumbling; M. Horowitz (2019). *Quantum computing: progress and prospects*. National Academies of Sciences, Engineering, and Medicine. p. 2. doi:10.17226/25196 (https://doi.org/10.17226%2F25196). ISBN 978-0-309-47969-1. S2CID 125635007 (https://api.semanticscholar.org/CorpusID:125635007).
5. T. Sleator; H. Weinfurter (1995). "Realizable Universal Quantum Logic Gates". *Physical Review Letters*. **74** (20): 4087–4090. Bibcode:1995PhRvL..74.4087S (https://ui.adsabs.harvard.edu/abs/1995PhRvL..74.4087S). doi:10.1103/PhysRevLett.74.4087 (https://doi.org/10.1103%2FPhysRevLett.74.4087). PMID 10058409 (https://pubmed.ncbi.nlm.nih.gov/10058409).
6. T. Hey (1999). "Quantum computing: An introduction". *Computing & Control Engineering Journal*. **10** (3): 105–112. doi:10.1049/cce:19990303 (https://doi.org/10.1049%2Fcce%3A19990303).
7. P. Shor (1998). *Quantum Computing* (http://nozdr.ru/data/media/biblio/kolxoz/M/ICM-1998,%20Berlin.%20Proceedings,%20Vol.%201%20Plenary%20lectures%20(no%20p.%2023-52)%20(Documenta%20Mathematica,%201998)(660s)_M_.pdf#page=434) (PDF). Documenta Mathematica. p. 468.
8. G.K. Brennen; C.M. Caves; P.S. Jessen; I.H. Deutsch (1999). "Quantum Logic Gates in Optical Lattices". *Physical Review Letters*. **82** (5): 1060–1063. arXiv:quant-ph/9806021 (https://arxiv.org/abs/quant-ph/9806021). Bibcode:1999PhRvL..82.1060B (https://ui.adsabs.harvard.edu/abs/1999PhRvL..82.1060B). doi:10.1103/PhysRevLett.82.1060 (https://doi.org/10.1103%2FPhysRevLett.82.1060). S2CID 15297433 (https://api.semanticscholar.org/CorpusID:15297433).
9. A. Barenco; C.H. Bennett; R. Cleve; D.P. DiVincenzo; N. Margolus; P. Shor; T. Sleator; J. Smolin; H. Weinfurter (1995). "Elementary gates for quantum computation". *Physical Review A*. **74** (20): 3457–3467. arXiv:quant-ph/9503016 (https://arxiv.org/abs/quant-ph/9503016). Bibcode:1995PhRvA..52.3457B (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.3457B). doi:10.1103/PhysRevA.52.3457 (https://doi.org/10.1103%2FPhysRevA.52.3457). PMID 9912645 (https://pubmed.ncbi.nlm.nih.gov/9912645). S2CID 8764584 (https://api.semanticscholar.org/CorpusID:8764584).
10. S. Lloyd (1995). "Almost Any Quantum Logic Gate is Universal". *Physical Review Letters*. **75** (2): 346–349. Bibcode:1995PhRvL..75..346L (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75..346L). doi:10.1103/PhysRevLett.75.346 (https://doi.org/10.1103%2FPhysRevLett.75.346). PMID 10059671 (https://pubmed.ncbi.nlm.nih.gov/10059671).
11. J. Joo; C.W. Lee; S. Kono; J. Kim (2019). "Logical measurement-based quantum computation in circuit-QED" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6851091). *Scientific Reports*. **9** (1): 16592. arXiv:1808.07638 (https://arxiv.org/abs/1808.07638). Bibcode:2019NatSR...916592J (https://ui.adsabs.harvard.edu/abs/2019NatSR...916592J). doi:10.1038/s41598-019-52866-3 (https://doi.org/10.1038%2Fs41598-019-52866-3). PMC 6851091 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6851091). PMID 31719588 (https://pubmed.ncbi.nlm.nih.gov/31719588). S2CID 119440765 (https://api.semanticscholar.org/CorpusID:119440765).

12. M.S. Tame; R. Prevedel; M. Paternostro; P. Bohi; M.S. Kim; A. Zeilinger (2007). "Experimental realization of Deutsch's algorithm in a one-way quantum computer". *Physical Review Letters*. **98** (14): 140501. arXiv:quant-ph/0611186 (https://arxiv.org/abs/quant-ph/0611186). Bibcode:2007PhRvL..98n0501T (https://ui.adsabs.harvard.edu/abs/2007PhRvL..98n0501T). doi:10.1103/PhysRevLett.98.140501 (https://doi.org/10.1103%2FPhysRevLett.98.140501). PMID 17501253 (https://pubmed.ncbi.nlm.nih.gov/17501253). S2CID 21518741 (https://api.semanticscholar.org/CorpusID:21518741).
13. R. Raussendorf; D. E. Browne & H. J. Briegel (2003). "Measurement-based quantum computation with cluster states". *Physical Review A*. **68** (2): 022312. arXiv:quant-ph/0301052 (https://arxiv.org/abs/quant-ph/0301052). Bibcode:2003PhRvA..68b2312R (https://ui.adsabs.harvard.edu/abs/2003PhRvA..68b2312R). doi:10.1103/PhysRevA.68.022312 (https://doi.org/10.1103%2FPhysRevA.68.022312). S2CID 6197709 (https://api.semanticscholar.org/CorpusID:6197709).
14. P. Walther; K. J. Resch; T. Rudolph; E. Schenck; H. Weinfurter; V. Vedral; M. Aspelmeyer; A. Zeilinger (2005). "Experimental one-way quantum computing". *Nature*. **434** (7030): 169–176. arXiv:quant-ph/0503126 (https://arxiv.org/abs/quant-ph/0503126). Bibcode:2005Natur.434..169W (https://ui.adsabs.harvard.edu/abs/2005Natur.434..169W). doi:10.1038/nature03347 (https://doi.org/10.1038%2Fnature03347). PMID 15758991 (https://pubmed.ncbi.nlm.nih.gov/15758991). S2CID 119329998 (https://api.semanticscholar.org/CorpusID:119329998).
15. R. Raussendorf & H. J. Briegel (2006). "A One-Way Quantum Computer". *Physical Review Letters*. **86** (22): 5188–91. arXiv:quant-ph/0510135 (https://arxiv.org/abs/quant-ph/0510135). Bibcode:2001PhRvL..86.5188R (https://ui.adsabs.harvard.edu/abs/2001PhRvL..86.5188R). doi:10.1103/PhysRevLett.86.5188 (https://doi.org/10.1103%2FPhysRevLett.86.5188). PMID 11384453 (https://pubmed.ncbi.nlm.nih.gov/11384453).
16. V. Danos; E. Kashefi; P. Panangaden (2007). "The measurement calculus". *Journal of the ACM*. **54** (2): 8. arXiv:0704.1263 (https://arxiv.org/abs/0704.1263). doi:10.1145/1219092.1219096 (https://doi.org/10.1145%2F1219092.1219096). S2CID 5851623 (https://api.semanticscholar.org/CorpusID:5851623).
17. E. Pius (2010). "Automatic Parallelisation of Quantum Circuits Using the Measurement Based Quantum Computing Model" (https://static.epcc.ed.ac.uk/dissertations/hpc-msc/2009-2010/Einar%20Pius.pdf) (PDF). `{{cite journal}}`: Cite journal requires `|journal=` (help)
18. A. Mantri; T.F. Demarie; J.F. Fitzsimons (2017). "Universality of quantum computation with cluster states and (X, Y)-plane measurements" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5316959). *Scientific Reports*. **7** (1): 42861. arXiv:1607.00758 (https://arxiv.org/abs/1607.00758). Bibcode:2017NatSR...742861M (https://ui.adsabs.harvard.edu/abs/2017NatSR...742861M). doi:10.1038/srep42861 (https://doi.org/10.1038%2Fsrep42861). PMC 5316959 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5316959). PMID 28216652 (https://pubmed.ncbi.nlm.nih.gov/28216652).
19. S. Anders; H.J. Briegel (2006). "Fast simulation of stabilizer circuits using a graph state representation". *Physical Review A*. **73** (2): 022334. arXiv:quant-ph/0504117 (https://arxiv.org/abs/quant-ph/0504117). Bibcode:2006PhRvA..73b2334A (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73b2334A). doi:10.1103/PhysRevA.73.022334 (https://doi.org/10.1103%2FPhysRevA.73.022334). S2CID 12763101 (https://api.semanticscholar.org/CorpusID:12763101).
20. T. Nutz; A. Milne; P. Shadbolt; T. Rudolph (2017). "Proposal for demonstration of long-range cluster state entanglement in the presence of photon loss". *APL Photonics*. **2** (6): 066103. arXiv:1702.01958 (https://arxiv.org/abs/1702.01958). Bibcode:2017APLP....2f6103N (https://ui.adsabs.harvard.edu/abs/2017APLP....2f6103N). doi:10.1063/1.4983822 (https://doi.org/10.1063%2F1.4983822). S2CID 125732242 (https://api.semanticscholar.org/CorpusID:125732242).

21. M. Gimeno-Segovia; P. Shadbolt; D.E. Browne; T. Rudolph (2015). "From Three-Photon Greenberger-Horne-Zeilinger States to Ballistic Universal Quantum Computation". *Physical Review Letters*. **115** (2): 020502. arXiv:1410.3720 (https://arxiv.org/abs/1410.3720). Bibcode:2015PhRvL.115b0502G (https://ui.adsabs.harvard.edu/abs/2015PhRvL.115b0502G). doi:10.1103/PhysRevLett.115.020502 (https://doi.org/10.1103%2FPhysRevLett.115.020502). PMID 26207455 (https://pubmed.ncbi.nlm.nih.gov/26207455). S2CID 45848374 (https://api.semanticscholar.org/CorpusID:45848374).
22. J.R. Scott; K.C. Balram (2022). "Timing Constraints Imposed by Classical Digital Control Systems on Photonic Implementations of Measurement-Based Quantum Computing". *IEEE Transactions on Quantum Engineering*. **3**: 1–20. arXiv:2109.04792 (https://arxiv.org/abs/2109.04792). doi:10.1109/TQE.2022.3175587 (https://doi.org/10.1109%2FTQE.2022.3175587). S2CID 237485449 (https://api.semanticscholar.org/CorpusID:237485449).
23. R. Jozsa (2006). "An introduction to measurement based quantum computation". *NATO Science Series, III: Computer and Systems Sciences. Quantum Information Processing-From Theory to Experiment*. **199**. arXiv:quant-ph/0508124 (https://arxiv.org/abs/quant-ph/0508124).
24. R. Raussendorf; H. J. Briegel (2002). "Computational model underlying the one-way quantum computer". arXiv:quant-ph/0108067 (https://arxiv.org/abs/quant-ph/0108067).
25. "OneQubitEulerDecomposer" (https://qiskit.org/documentation/stubs/qiskit.quantum_info.OneQubitEulerDecomposer.html). *Qiskit*. Retrieved 29 June 2022.
26. "MBQC Quick Start Guide" (https://qml.baidu.com/tutorials/measurement-based-quantum-computation/mbqc-quick-start-guide.html). *Paddle Quantum*. Retrieved 29 June 2022.
27. "Measurement-Based Quantum Computation Module" (https://qml.baidu.com/tutorials/measurement-based-quantum-computation/measurement-based-quantum-computation-module.html). *Paddle Quantum*. Retrieved 1 July 2022.
28. K. Fujii (2015). *Quantum Computation with Topological Codes: from qubit to topological fault-tolerance*. Springer. p. 28. arXiv:1504.01444 (https://arxiv.org/abs/1504.01444). ISBN 978-981-287-996-7.
29. D. Gottesman (1998). "The Heisenberg Representation of Quantum Computers". arXiv:quant-ph/9807006 (https://arxiv.org/abs/quant-ph/9807006). Bibcode:1998quant.ph..7006G (https://ui.adsabs.harvard.edu/abs/1998quant.ph..7006G).
    `{{cite journal}}`: Cite journal requires `|journal=` (help)
30. M. Hein; W. Dur; J. Eisert; R. Raussendorf; M. Van den Nest; H. Jurgen Briegel (2006). "Entanglement in Graph States and its Applications". arXiv:quant-ph/0602096 (https://arxiv.org/abs/quant-ph/0602096).
31. R. Raussendorf; J. Harrington; K. Goyal (2006). "A fault-tolerant one-way quantum computer". *Annals of Physics*. **321** (9): 2242–2270. arXiv:quant-ph/0510135 (https://arxiv.org/abs/quant-ph/0510135). Bibcode:2006AnPhy.321.2242R (https://ui.adsabs.harvard.edu/abs/2006AnPhy.321.2242R). doi:10.1016/j.aop.2006.01.012 (https://doi.org/10.1016%2Fj.aop.2006.01.012). S2CID 14422769 (https://api.semanticscholar.org/CorpusID:14422769).
32. M. Rossi; M. Huber; D. Bruß; C. Macchiavello (2013). "Quantum Hypergraph States". *New Journal of Physics*. **15** (11): 113022. arXiv:1211.5554 (https://arxiv.org/abs/1211.5554). Bibcode:2013NJPh...15k3022R (https://ui.adsabs.harvard.edu/abs/2013NJPh...15k3022R). doi:10.1088/1367-2630/15/11/113022 (https://doi.org/10.1088%2F1367-2630%2F15%2F11%2F113022). S2CID 40507835 (https://api.semanticscholar.org/CorpusID:40507835).
33. M.E. Cuffaro (2013). "On the Significance of the Gottesman–Knill Theorem". *The British Journal for the Philosophy of Science*. **68** (1): 91–121. arXiv:1310.0938 (https://arxiv.org/abs/1310.0938). doi:10.1093/bjps/axv016 (https://doi.org/10.1093%2Fbjps%2Faxv016).
34. K. Fujii (2015). *Quantum Computation with Topological Codes: from qubit to topological fault-tolerance*. Springer. p. 30. arXiv:1504.01444 (https://arxiv.org/abs/1504.01444). ISBN 978-981-287-996-7.

35. K. Fujii (2015). *Quantum Computation with Topological Codes: from qubit to topological fault-tolerance*. Springer. p. 34. arXiv:1504.01444 (https://arxiv.org/abs/1504.01444). ISBN 978-981-287-996-7.
36. M.A. Nielsen; I.L. Chuang (2000). *Quantum Computation and Quantum Information*. Cambridge University Press. p. 464. ISBN 978-1-107-00217-3.
37. M. Van den Nest (2008). "Classical simulation of quantum computation, the Gottesman-Knill theorem, and slightly beyond". *Quantum Information & Computation*. **10** (3). arXiv:0811.0898 (https://arxiv.org/abs/0811.0898).
38. Robert Raussendorf; Jim Harrington; Kovid Goyal (2007). "Topological fault-tolerance in cluster state quantum computation". *New Journal of Physics*. **9** (6): 199. arXiv:quant-ph/0703143 (https://arxiv.org/abs/quant-ph/0703143). Bibcode:2007NJPh....9..199R (https://ui.adsabs.harvard.edu/abs/2007NJPh....9..199R). doi:10.1088/1367-2630/9/6/199 (https://doi.org/10.1088%2F1367-2630%2F9%2F6%2F199). S2CID 13811487 (https://api.semanticscholar.org/CorpusID:13811487).
39. Robert Raussendorf; Jim Harrington (2007). "Fault-tolerant quantum computation with high threshold in two dimensions". *Physical Review Letters*. **98** (19): 190504. arXiv:quant-ph/0610082 (https://arxiv.org/abs/quant-ph/0610082). Bibcode:2007PhRvL..98s0504R (https://ui.adsabs.harvard.edu/abs/2007PhRvL..98s0504R). doi:10.1103/physrevlett.98.190504 (https://doi.org/10.1103%2Fphysrevlett.98.190504). PMID 17677613 (https://pubmed.ncbi.nlm.nih.gov/17677613). S2CID 39504821 (https://api.semanticscholar.org/CorpusID:39504821).
40. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger (2005). "Experimental one-way quantum computing". *Nature*. **434** (7030): 169–76. arXiv:quant-ph/0503126 (https://arxiv.org/abs/quant-ph/0503126). Bibcode:2005Natur.434..169W (https://ui.adsabs.harvard.edu/abs/2005Natur.434..169W). doi:10.1038/nature03347 (https://doi.org/10.1038%2Fnature03347). PMID 15758991 (https://pubmed.ncbi.nlm.nih.gov/15758991). S2CID 119329998 (https://api.semanticscholar.org/CorpusID:119329998).
41. Robert Prevedel; Philip Walther; Felix Tiefenbacher; Pascal Böhi; Rainer Kaltenbaek; Thomas Jennewein; Anton Zeilinger (2007). "High-speed linear optics quantum computing using active feed-forward". *Nature*. **445** (7123): 65–69. arXiv:quant-ph/0701017 (https://arxiv.org/abs/quant-ph/0701017). Bibcode:2007Natur.445...65P (https://ui.adsabs.harvard.edu/abs/2007Natur.445...65P). doi:10.1038/nature05346 (https://doi.org/10.1038%2Fnature05346). PMID 17203057 (https://pubmed.ncbi.nlm.nih.gov/17203057). S2CID 4416906 (https://api.semanticscholar.org/CorpusID:4416906).
42. Daniel E. Browne; Terry Rudolph (2005). "Resource-efficient linear optical quantum computation". *Physical Review Letters*. **95** (1): 010501. arXiv:quant-ph/0405157 (https://arxiv.org/abs/quant-ph/0405157). Bibcode:2005PhRvL..95a0501B (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95a0501B). doi:10.1103/PhysRevLett.95.010501 (https://doi.org/10.1103%2FPhysRevLett.95.010501). PMID 16090595 (https://pubmed.ncbi.nlm.nih.gov/16090595). S2CID 27224760 (https://api.semanticscholar.org/CorpusID:27224760).
43. Olaf Mandel; Markus Greiner; Artur Widera; Tim Rom; Theodor W. Hänsch; Immanuel Bloch (2003). "Controlled collisions for multi-particle entanglement of optically trapped atoms". *Nature*. **425** (6961): 937–40. arXiv:quant-ph/0308080 (https://arxiv.org/abs/quant-ph/0308080). Bibcode:2003Natur.425..937M (https://ui.adsabs.harvard.edu/abs/2003Natur.425..937M). doi:10.1038/nature02008 (https://doi.org/10.1038%2Fnature02008). PMID 14586463 (https://pubmed.ncbi.nlm.nih.gov/14586463). S2CID 4408587 (https://api.semanticscholar.org/CorpusID:4408587).

44. Tzu-Chieh Wei; Ian Affleck & Robert Raussendorf (2012). "Two-dimensional Affleck-Kennedy-Lieb-Tasaki state on the honeycomb lattice is a universal resource for quantum computation". *Physical Review A*. **86** (32328): 032328. arXiv:1009.2840 (https://arxiv.org/abs/1009.2840). Bibcode:2012PhRvA..86c2328W (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86c2328W). doi:10.1103/PhysRevA.86.032328 (https://doi.org/10.1103%2FPhysRevA.86.032328). S2CID 118128175 (https://api.semanticscholar.org/CorpusID:118128175).
45. Akimasa Miyake (2011). "Quantum computational capability of a 2D valence bond solid phase". *Annals of Physics*. **236** (7): 1656–1671. arXiv:1009.3491 (https://arxiv.org/abs/1009.3491). Bibcode:2011AnPhy.326.1656M (https://ui.adsabs.harvard.edu/abs/2011AnPhy.326.1656M). doi:10.1016/j.aop.2011.03.006 (https://doi.org/10.1016%2Fj.aop.2011.03.006). S2CID 119243954 (https://api.semanticscholar.org/CorpusID:119243954).
46. Tzu-Chieh Wei; Poya Haghnegahdar; Robert Raussendorf (2014). "Spin mixture AKLT states for universal quantum computation". *Physical Review A*. **90** (4): 042333. arXiv:1310.5100 (https://arxiv.org/abs/1310.5100). Bibcode:2014PhRvA..90d2333W (https://ui.adsabs.harvard.edu/abs/2014PhRvA..90d2333W). doi:10.1103/PhysRevA.90.042333 (https://doi.org/10.1103%2FPhysRevA.90.042333). S2CID 118460519 (https://api.semanticscholar.org/CorpusID:118460519).

General

- D. Gross; J. Eisert; N. Schuch; D. Perez-Garcia (2007). "Measurement-based quantum computation beyond the one-way model". *Physical Review A*. **76** (5): 052315. arXiv:0706.3401 (https://arxiv.org/abs/0706.3401). Bibcode:2007PhRvA..76e2315G (https://ui.adsabs.harvard.edu/abs/2007PhRvA..76e2315G). doi:10.1103/PhysRevA.76.052315 (https://doi.org/10.1103%2FPhysRevA.76.052315). S2CID 53409763 (https://api.semanticscholar.org/CorpusID:53409763). Non-cluster resource states
- A. Trisetyarso & R. Van Meter (2010). "Circuit Design for A Measurement-Based Quantum Carry-Lookahead Adder". *International Journal of Quantum Information*. **8** (5): 843–867. arXiv:0903.0748 (https://arxiv.org/abs/0903.0748). doi:10.1142/S0219749910006496 (https://doi.org/10.1142%2FS0219749910006496). S2CID 2587811 (https://api.semanticscholar.org/CorpusID:2587811). Measurement-based quantum computation, quantum carry-lookahead adder

---

Retrieved from "https://en.wikipedia.org/w/index.php?title=One-way_quantum_computer&oldid=1243063086"

WIKIPEDIA
The Free Encyclopedia

Cluster state

In quantum information and quantum computing, a **cluster state**[1] is a type of highly entangled state of multiple qubits. Cluster states are generated in lattices of qubits with Ising type interactions. A cluster *C* is a connected subset of a *d*-dimensional lattice, and a cluster state is a pure state of the qubits located on *C*. They are different from other types of entangled states such as GHZ states or W states in that it is more difficult to eliminate quantum entanglement (via projective measurements) in the case of cluster states. Another way of thinking of cluster states is as a particular instance of graph states, where the underlying graph is a connected subset of a *d*-dimensional lattice. Cluster states are especially useful in the context of the one-way quantum computer. For a comprehensible introduction to the topic see.[2]

Formally, cluster states $|\phi_{\{\kappa\}}\rangle_C$ are states which obey the set eigenvalue equations:

$$K^{(a)}|\phi_{\{\kappa\}}\rangle_C = (-1)^{\kappa_a}|\phi_{\{\kappa\}}\rangle_C$$

where $K^{(a)}$ are the correlation operators

$$K^{(a)} = \sigma_x^{(a)} \bigotimes_{b \in \mathrm{N}(a)} \sigma_z^{(b)}$$

with σ_x and σ_z being Pauli matrices, $N(a)$ denoting the neighbourhood of a and $\{\kappa_a \in \{0,1\} | a \in C\}$ being a set of binary parameters specifying the particular instance of a cluster state.

Examples with qubits

Here are some examples of one-dimensional cluster states (*d*=1), for $n = 2, 3, 4$, where n is the number of qubits. We take $\kappa_a = 0$ for all a, which means the cluster state is the unique simultaneous eigenstate that has corresponding eigenvalue 1 under all correlation operators. In each example the set of correlation operators $\{K^{(a)}\}_a$and the corresponding cluster state is listed.

- $n = 2$
  $\{\sigma_x\sigma_z,\ \sigma_z\sigma_x\}$

  $|\phi\rangle = \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)$
  This is an EPR-pair (up to local transformations).

- $n = 3$

  $\{\sigma_x\sigma_z I,\ \sigma_z\sigma_x\sigma_z,\ I\sigma_z\sigma_x\}$
  $|\phi\rangle = \frac{1}{\sqrt{2}}(|+0+\rangle + |-1-\rangle)$
  This is the GHZ-state (up to local transformations).

- $n = 4$

  $\{\sigma_x\sigma_z II,\ \sigma_z\sigma_x\sigma_z I,\ I\sigma_z\sigma_x\sigma_z,\ II\sigma_z\sigma_x\}$
  $|\phi\rangle = \frac{1}{2}(|+0+0\rangle + |+0-1\rangle + |-1-0\rangle + |-1+1\rangle)$.
  This is not a GHZ-state and can not be converted to a GHZ-state with local operations.

In all examples I is the identity operator, and tensor products are omitted. The states above can be obtained from the all zero state $|0\ldots0\rangle$ by first applying a Hadamard gate to every qubit, and then a controlled-Z gate between all qubits that are adjacent to each other.

Experimental creation of cluster states

Cluster states can be realized experimentally. One way to create a cluster state is by encoding logical qubits into the polarization of photons, one common encoding is the following:

$$\begin{cases} |0\rangle_{\mathrm{L}} \longleftrightarrow |\mathrm{H}\rangle \\ |1\rangle_{\mathrm{L}} \longleftrightarrow |\mathrm{V}\rangle \end{cases}$$

This is not the only possible encoding, however it is one of the simplest: with this encoding entangled pairs can be created experimentally through spontaneous parametric down-conversion.[3][4] The entangled pairs that can be generated this way have the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\mathrm{H}\rangle|\mathrm{H}\rangle + \mathrm{e}^{\mathrm{i}\phi}|\mathrm{V}\rangle|\mathrm{V}\rangle\right)$$

equivalent to the logical state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + e^{i\phi}|1\rangle|1\rangle\right)$$

for the two choices of the phase $\phi = 0, \pi$ the two Bell states $|\Phi^+\rangle, |\Phi^-\rangle$ are obtained: these are themselves two examples of two-qubits cluster states. Through the use of linear optic devices as beam-splitters or wave-plates these Bell states can interact and form more complex cluster states.[5] Cluster states have been created also in optical lattices of cold atoms.[6]

Entanglement criteria and Bell inequalities for cluster states

After a cluster state was created in an experiment, it is important to verify that indeed, an entangled quantum state has been created. The fidelity with respect to the N-qubit cluster state $|C_N\rangle$ is given by

$$F_{CN} = \mathrm{Tr}(\rho|C_N\rangle\langle C_N|),$$

It has been shown that if $F_{CN} > 1/2$, then the state ρ has genuine multiparticle entanglement.[7] Thus, one can obtain an entanglement witness detecting entanglement close the cluster states as

$$W_{CN} = \frac{1}{2}\mathbf{Identity} - |C_N\rangle\langle C_N|.$$

where $\langle W_{CN} \rangle < 0$ signals genuine multiparticle entanglement.

Such a witness cannot be measured directly. It has to be decomposed to a sum of correlations terms, which can then be measured. However, for large systems this approach can be difficult.

There are also entanglement witnesses that work in very large systems, and they also detect genuine multipartite entanglement close to cluster states. They need only the minimal two local measurement settings.[7] Similar conditions can also be used to put a lower bound on the fidelity with respect to an ideal cluster state.[8] These criteria have been used first in an experiment realizing four-qubit cluster states with photons.[4] These approaches have also been used to propose methods for detecting entanglement in a smaller part of a large cluster state or graph state realized in optical lattices.[9]

Bell inequalities have also been developed for cluster states.[10] [11] [12] All these entanglement conditions and Bell inequalities are based on the stabilizer formalism.[13]

See also

- Bell state
- Graph state
- Optical cluster state

References

1. H. J. Briegel; R. Raussendorf (2001). "Persistent Entanglement in arrays of Interacting Particles". *Physical Review Letters*. **86** (5): 910–3. arXiv:quant-ph/0004051 (https://arxiv.org/abs/quant-ph/0004051). Bibcode:2001PhRvL..86..910B (https://ui.adsabs.harvard.edu/abs/2001PhRvL..86..910B). doi:10.1103/PhysRevLett.86.910 (https://doi.org/10.1103%2FPhysRevLett.86.910). PMID 11177971 (https://pubmed.ncbi.nlm.nih.gov/11177971). S2CID 21762622 (https://api.semanticscholar.org/CorpusID:21762622).
2. Briegel, Hans J. (12 August 2009). "Cluster States". In Greenberger, Daniel; Hentschel, Klaus & Weinert, Friedel (eds.). *Compendium of Quantum Physics - Concepts, Experiments, History and Philosophy*. Springer. pp. 96–105. ISBN 978-3-540-70622-9.
3. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger (2005). "Experimental one-way quantum computing". *Nature*. **434** (7030): 169–76. arXiv:quant-ph/0503126 (https://arxiv.org/abs/quant-ph/0503126). Bibcode:2005Natur.434..169W (https://ui.adsabs.harvard.edu/abs/2005Natur.434..169W). doi:10.1038/nature03347 (https://doi.org/10.1038%2Fnature03347). PMID 15758991 (https://pubmed.ncbi.nlm.nih.gov/15758991). S2CID 119329998 (https://api.semanticscholar.org/CorpusID:119329998).
4. N. Kiesel; C. Schmid; U. Weber; G. Tóth; O. Gühne; R. Ursin; H. Weinfurter (2005). "Experimental Analysis of a 4-Qubit Cluster State". *Phys. Rev. Lett*. **95** (21): 210502. arXiv:quant-ph/0508128 (https://arxiv.org/abs/quant-ph/0508128). Bibcode:2005PhRvL..95u0502K (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95u0502K). doi:10.1103/PhysRevLett.95.210502 (https://doi.org/10.1103%2FPhysRevLett.95.210502). PMID 16384122 (https://pubmed.ncbi.nlm.nih.gov/16384122). S2CID 5322108 (https://api.semanticscholar.org/CorpusID:5322108).

5. Zhang, An-Ning; Lu, Chao-Yang; Zhou, Xiao-Qi; Chen, Yu-Ao; Zhao, Zhi; Yang, Tao; Pan, Jian-Wei (2006-02-17). "Experimental construction of optical multiqubit cluster states from Bell states" (https://link.aps.org/doi/10.1103/PhysRevA.73.022330). *Physical Review A*. **73** (2): 022330. arXiv:quant-ph/0501036 (https://arxiv.org/abs/quant-ph/0501036). Bibcode:2006PhRvA..73b2330Z (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73b2330Z). doi:10.1103/PhysRevA.73.022330 (https://doi.org/10.1103%2FPhysRevA.73.022330). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 118882320 (https://api.semanticscholar.org/CorpusID:118882320).
6. O. Mandel; M. Greiner; A. Widera; T. Rom; T. W. Hänsch; I. Bloch (2003). "Controlled collisions for multi-particle entanglement of optically trapped atoms". *Nature*. **425** (6961): 937–940. arXiv:quant-ph/0308080 (https://arxiv.org/abs/quant-ph/0308080). Bibcode:2003Natur.425..937M (https://ui.adsabs.harvard.edu/abs/2003Natur.425..937M). doi:10.1038/nature02008 (https://doi.org/10.1038%2Fnature02008). PMID 14586463 (https://pubmed.ncbi.nlm.nih.gov/14586463). S2CID 4408587 (https://api.semanticscholar.org/CorpusID:4408587).
7. Tóth, Géza; Gühne, Otfried (17 February 2005). "Detecting Genuine Multipartite Entanglement with Two Local Measurements". *Physical Review Letters*. **94** (6): 060501. arXiv:quant-ph/0405165 (https://arxiv.org/abs/quant-ph/0405165). Bibcode:2005PhRvL..94f0501T (https://ui.adsabs.harvard.edu/abs/2005PhRvL..94f0501T). doi:10.1103/PhysRevLett.94.060501 (https://doi.org/10.1103%2FPhysRevLett.94.060501). PMID 15783712 (https://pubmed.ncbi.nlm.nih.gov/15783712). S2CID 13371901 (https://api.semanticscholar.org/CorpusID:13371901).
8. Tóth, Géza; Gühne, Otfried (29 August 2005). "Entanglement detection in the stabilizer formalism". *Physical Review A*. **72** (2): 022340. arXiv:quant-ph/0501020 (https://arxiv.org/abs/quant-ph/0501020). Bibcode:2005PhRvA..72b2340T (https://ui.adsabs.harvard.edu/abs/2005PhRvA..72b2340T). doi:10.1103/PhysRevA.72.022340 (https://doi.org/10.1103%2FPhysRevA.72.022340). S2CID 56269409 (https://api.semanticscholar.org/CorpusID:56269409).
9. Alba, Emilio; Tóth, Géza; García-Ripoll, Juan José (21 December 2010). "Mapping the spatial distribution of entanglement in optical lattices". *Physical Review A*. **82** (6). arXiv:1007.0985 (https://arxiv.org/abs/1007.0985). doi:10.1103/PhysRevA.82.062321 (https://doi.org/10.1103%2FPhysRevA.82.062321).
10. Scarani, Valerio; Acín, Antonio; Schenck, Emmanuel; Aspelmeyer, Markus (18 April 2005). "Nonlocality of cluster states of qubits" (https://archive-ouverte.unige.ch/unige:47355). *Physical Review A*. **71** (4): 042325. arXiv:quant-ph/0405119 (https://arxiv.org/abs/quant-ph/0405119). Bibcode:2005PhRvA..71d2325S (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71d2325S). doi:10.1103/PhysRevA.71.042325 (https://doi.org/10.1103%2FPhysRevA.71.042325). S2CID 4805039 (https://api.semanticscholar.org/CorpusID:4805039).
11. Gühne, Otfried; Tóth, Géza; Hyllus, Philipp; Briegel, Hans J. (14 September 2005). "Bell Inequalities for Graph States". *Physical Review Letters*. **95** (12): 120405. arXiv:quant-ph/0410059 (https://arxiv.org/abs/quant-ph/0410059). Bibcode:2005PhRvL..95l0405G (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95l0405G). doi:10.1103/PhysRevLett.95.120405 (https://doi.org/10.1103%2FPhysRevLett.95.120405). PMID 16197057 (https://pubmed.ncbi.nlm.nih.gov/16197057). S2CID 5973814 (https://api.semanticscholar.org/CorpusID:5973814).
12. Tóth, Géza; Gühne, Otfried; Briegel, Hans J. (2 February 2006). "Two-setting Bell inequalities for graph states". *Physical Review A*. **73** (2): 022303. arXiv:quant-ph/0510007 (https://arxiv.org/abs/quant-ph/0510007). Bibcode:2006PhRvA..73b2303T (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73b2303T). doi:10.1103/PhysRevA.73.022303 (https://doi.org/10.1103%2FPhysRevA.73.022303). S2CID 108291031 (https://api.semanticscholar.org/CorpusID:108291031).

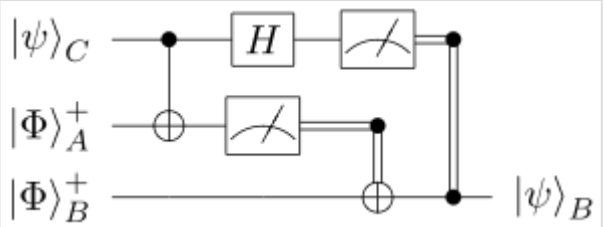
13. Gottesman, Daniel (1 September 1996). "Class of quantum error-correcting codes saturating the quantum Hamming bound". *Physical Review A*. **54** (3): 1862–1868. arXiv:quant-ph/9604038 (https://arxiv.org/abs/quant-ph/9604038). Bibcode:1996PhRvA..54.1862G (https://ui.adsabs.harvard.edu/abs/1996PhRvA..54.1862G). doi:10.1103/PhysRevA.54.1862 (https://doi.org/10.1103%2FPhysRevA.54.1862). PMID 9913672 (https://pubmed.ncbi.nlm.nih.gov/9913672). S2CID 16407184 (https://api.semanticscholar.org/CorpusID:16407184).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cluster_state&oldid=1224743256"

WIKIPEDIA
The Free Encyclopedia

Quantum circuit

In quantum information theory, a **quantum circuit** is a model for quantum computation, similar to classical circuits, in which a computation is a sequence of quantum gates, measurements, initializations of qubits to known values, and possibly other actions. The minimum set of actions that a circuit needs to be able to perform on the qubits to enable quantum computation is known as DiVincenzo's criteria.



Circuit that performs teleportation of a qubit.[1] This circuit consists of both quantum gates and measurements. Measurement is a quantum phenomenon that does not occur in classical circuits.

Circuits are written such that the horizontal axis is time, starting at the left hand side and ending at the right. Horizontal lines are qubits, doubled lines represent classical bits. The items that are connected by these lines are operations performed on the qubits, such as measurements or gates. These lines define the sequence of events, and are usually not physical cables.[2][3][4]

The graphical depiction of quantum circuit elements is described using a variant of the Penrose graphical notation. Richard Feynman used an early version of the quantum circuit notation in 1986.[5]

Reversible classical logic gates

Most elementary logic gates of a classical computer are not reversible. Thus, for instance, for an AND gate one cannot always recover the two input bits from the output bit; for example, if the output bit is 0, we cannot tell from this whether the input bits are 01 or 10 or 00.

However, reversible gates in classical computers are easily constructed for bit strings of any length; moreover, these are actually of practical interest, since irreversible gates must always increase physical entropy. A reversible gate is a reversible function on n-bit data that returns n-bit data, where an n-bit data is a string of bits $x_1,x_2, ...,x_n$ of length n. The set of n-bit data is the space $\{0,1\}^n$, which consists of 2^n strings of 0's and 1's.

More precisely: an n-bit reversible gate is a bijective mapping f from the set $\{0,1\}^n$ of n-bit data onto itself. An example of such a reversible gate f is a mapping that applies a fixed permutation to its inputs. For reasons of practical engineering, one typically studies gates only for small values of n, e.g. n=1, n=2 or n=3. These gates can be easily described by tables.

Quantum logic gates

The quantum logic gates are reversible unitary transformations on at least one qubit. Multiple qubits taken together are referred to as quantum registers. To define quantum gates, we first need to specify the quantum replacement of an *n*-bit datum. The *quantized version* of classical *n*-bit space $\{0,1\}^n$ is the Hilbert space

$$H_{\mathrm{QB}(n)} = \ell^2(\{0,1\}^n).$$

This is by definition the space of complex-valued functions on $\{0,1\}^n$ and is naturally an inner product space. ℓ^2 means the function is a square-integrable function. This space can also be regarded as consisting of linear combinations, or superpositions, of classical bit strings. Note that $H_{\mathrm{QB}(n)}$ is a vector space over the complex numbers of dimension 2^n. The elements of this vector space are the possible state-vectors of *n*-qubit quantum registers.

Using Dirac ket notation, if $x_1, x_2, \ldots, x_n$ is a classical bit string, then

$$|x_1, x_2, \cdots, x_n\rangle$$

is a special *n*-qubit register corresponding to the function which maps this classical bit string to 1 and maps all other bit strings to 0; these 2^n special *n*-qubit registers are called *computational basis states*. All *n*-qubit registers are complex linear combinations of these computational basis states.

Quantum logic gates, in contrast to classical logic gates, are always reversible. One requires a special kind of reversible function, namely a unitary mapping, that is, a linear transformation of a complex inner product space that preserves the Hermitian inner product. An *n*-qubit (reversible) quantum gate is a unitary mapping *U* from the space $H_{\mathrm{QB}(n)}$ of *n*-qubit registers onto itself.

Typically, we are only interested in gates for small values of *n*.

A reversible *n*-bit classical logic gate gives rise to a reversible *n*-bit quantum gate as follows: to each reversible *n*-bit logic gate *f* corresponds a quantum gate W_f defined as follows:

$$W_f(|x_1, x_2, \cdots, x_n\rangle) = |f(x_1, x_2, \cdots, x_n)\rangle.$$

Note that W_f permutes the computational basis states.

Of particular importance is the controlled NOT gate (also called CNOT gate) W_{CNOT} defined on a quantized 2 qubit. Other examples of quantum logic gates derived from classical ones are the Toffoli gate and the Fredkin gate.

However, the Hilbert-space structure of the qubits permits many quantum gates that are not induced by classical ones. For example, a relative phase shift is a 1 qubit gate given by multiplication by the phase shift operator:

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix},$$

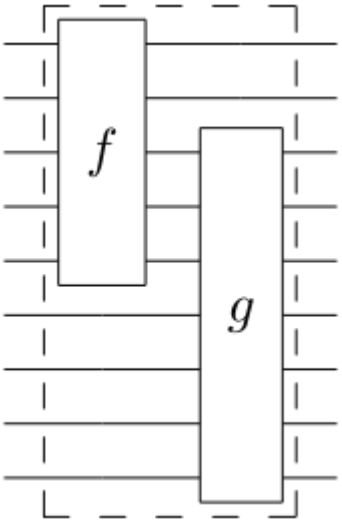
so

$$P(\varphi)|0\rangle = |0\rangle \quad P(\varphi)|1\rangle = e^{i\varphi}|1\rangle.$$

Reversible logic circuits

Again, we consider first *reversible* classical computation. Conceptually, there is no difference between a reversible *n*-bit circuit and a reversible *n*-bit logic gate: either one is just an invertible function on the space of *n* bit data. However, as mentioned in the previous section, for engineering reasons we would like to have a small number of simple reversible gates, that can be put together to assemble any reversible circuit.

To explain this assembly process, suppose we have a reversible *n*-bit gate *f* and a reversible *m*-bit gate *g*. Putting them together means producing a new circuit by connecting some set of *k* outputs of *f* to some set of *k* inputs of *g* as in the figure below. In that figure, *n*=5, *k*=3 and *m*=7. The resulting circuit is also reversible and operates on *n*+*m*−*k* bits.



We will refer to this scheme as a *classical assemblage* (This concept corresponds to a technical definition in Kitaev's pioneering paper cited below). In composing these reversible machines, it is important to ensure that the intermediate machines are also reversible. This condition assures that *intermediate* "garbage" is not created (the net physical effect would be to increase entropy, which is one of the motivations for going through this exercise).

Note that each horizontal line on the above picture represents either 0 or 1, not these probabilities. Since quantum computations are reversible, at each 'step' the number of lines must be the same number of input lines. Also, each input combination must be mapped to a single combination at each 'step'. This means that each intermediate combination in a quantum circuit is a bijective function of the input.[6]

Now it is possible to show that the Toffoli gate is a universal gate. This means that given any reversible classical *n*-bit circuit *h*, we can construct a classical assemblage of Toffoli gates in the above manner to produce an (*n*+*m*)-bit circuit *f* such that

$$f(x_1, \ldots, x_n, \underbrace{0, \ldots, 0}) = (y_1, \ldots, y_n, \underbrace{0, \ldots, 0})$$

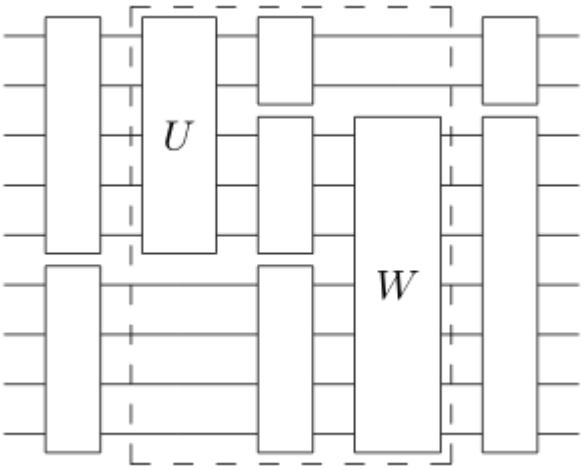
where there are *m* underbraced zeroed inputs and

$$(y_1, \ldots, y_n) = h(x_1, \ldots, x_n).$$

Notice that the result always has a string of *m* zeros as the ancilla bits. No "rubbish" is ever produced, and so this computation is indeed one that, in a physical sense, generates no entropy. This issue is carefully discussed in Kitaev's article.

More generally, any function *f* (bijective or not) can be simulated by a circuit of Toffoli gates. Obviously, if the mapping fails to be injective, at some point in the simulation (for example as the last step) some "garbage" has to be produced.

For quantum circuits a similar composition of qubit gates can be defined. That is, associated to any *classical assemblage* as above, we can produce a reversible quantum circuit when in place of *f* we have an *n*-qubit gate *U* and in place of *g* we have an *m*-qubit gate *W*. See illustration below:



The fact that connecting gates this way gives rise to a unitary mapping on $n+m-k$ qubit space is easy to check. In a real quantum computer the physical connection between the gates is a major engineering challenge, since it is one of the places where decoherence may occur.

There are also universality theorems for certain sets of well-known gates; such a universality theorem exists, for instance, for the pair consisting of the single qubit phase gate U_θ mentioned above (for a suitable value of θ), together with the 2-qubit CNOT gate W_{CNOT}. However, the universality theorem for the quantum case is somewhat weaker than the one for the classical case; it asserts only that any reversible *n*-qubit circuit can be *approximated* arbitrarily well by circuits assembled from these two elementary gates. Note that there are uncountably many possible single qubit phase gates, one for every possible angle θ, so they cannot all be represented by a finite circuit constructed from $\{U_\theta, W_{\text{CNOT}}\}$.

Quantum computations

So far we have not shown how quantum circuits are used to perform computations. Since many important numerical problems reduce to computing a unitary transformation *U* on a finite-dimensional space (the celebrated discrete Fourier transform being a prime example), one might expect that some quantum circuit could be designed to carry out the transformation *U*. In principle, one needs only to prepare an *n* qubit state ψ as an appropriate superposition of computational basis states for the input and measure the output $U\psi$. Unfortunately, there are two problems with this:

- One cannot measure the phase of ψ at any computational basis state so there is no way of reading out the complete answer. This is in the nature of measurement in quantum mechanics.
- There is no way to efficiently prepare the input state ψ.

This does not prevent quantum circuits for the discrete Fourier transform from being used as intermediate steps in other quantum circuits, but the use is more subtle. In fact quantum computations are *probabilistic*.

We now provide a mathematical model for how quantum circuits can simulate *probabilistic* but classical computations. Consider an *r*-qubit circuit *U* with register space $H_{\mathrm{QB}(r)}$. *U* is thus a unitary map

$$H_{\mathrm{QB}(r)} \to H_{\mathrm{QB}(r)}.$$

In order to associate this circuit to a classical mapping on bitstrings, we specify

- An *input register* $X = \{0,1\}^m$ of *m* (classical) bits.
- An *output register* $Y = \{0,1\}^n$ of *n* (classical) bits.

The contents $x = x_1, ..., x_m$ of the classical input register are used to initialize the qubit register in some way. Ideally, this would be done with the computational basis state

$$|\vec{x}, 0\rangle = |x_1, x_2, \cdots, x_m, \underbrace{0, \ldots, 0}\rangle,$$

where there are *r-m* underbraced zeroed inputs. Nevertheless, this perfect initialization is completely unrealistic. Let us assume therefore that the initialization is a mixed state given by some density operator *S* which is near the idealized input in some appropriate metric, e.g.

$$\mathbf{Tr}\left(\left||\vec{x}, 0\rangle\langle\vec{x}, 0| - S\right|\right) \leq \delta.$$

Similarly, the output register space is related to the qubit register, by a *Y* valued observable *A*. Note that observables in quantum mechanics are usually defined in terms of *projection valued measures* on **R**; if the variable happens to be discrete, the projection valued measure reduces to a family $\{\mathrm{E}_\lambda\}$ indexed on some parameter λ ranging over a countable set. Similarly, a *Y* valued observable, can be associated with a family of pairwise orthogonal projections $\{\mathrm{E}_y\}$ indexed by elements of *Y*. such that

$$I = \sum_{y \in Y} \mathbf{E}_y.$$

Given a mixed state *S*, there corresponds a probability measure on *Y* given by

$$\mathbf{Pr}\{y\} = \mathbf{Tr}(S\,\mathbf{E}_y).$$

The function $F{:}X \to Y$ is computed by a circuit $U{:}H_{\mathrm{QB}(r)} \to H_{\mathrm{QB}(r)}$ to within ε if and only if for all bitstrings *x* of length *m*

$$\left\langle \vec{x}, 0 \middle| U^* \, \mathbf{E}_{F(x)} \, U \middle| \vec{x}, 0 \right\rangle = \left\langle \mathbf{E}_{F(x)} \, U(|\vec{x}, 0\rangle) \middle| U(|\vec{x}, 0\rangle) \right\rangle \geq 1 - \epsilon.$$

Now

$$\left|\mathbf{Tr}(SU^* \, \mathbf{E}_{F(x)} \, U) - \left\langle \vec{x}, 0 \right| U^* \, \mathbf{E}_{F(x)} \, U \left| \vec{x}, 0 \right\rangle\right| \leq \mathbf{Tr}(\left|\left|\vec{x}, 0\right\rangle\left\langle \vec{x}, 0\right| - S\right|)\|U^* \, \mathbf{E}_{F(x)} \, U\| \leq \delta$$

so that

$$\mathbf{Tr}(SU^* \, \mathbf{E}_{F(x)} \, U) \geq 1 - \epsilon - \delta.$$

Theorem. If ε + δ < 1/2, then the probability distribution

$$\mathbf{Pr}\{y\} = \mathbf{Tr}(SU^* \, \mathbf{E}_y \, U)$$

on *Y* can be used to determine *F*(*x*) with an arbitrarily small probability of error by majority sampling, for a sufficiently large sample size. Specifically, take *k* independent samples from the probability distribution Pr on *Y* and choose a value on which more than half of the samples agree. The probability that the value *F*(*x*) is sampled more than *k*/2 times is at least

$$1 - e^{-2\gamma^2 k},$$

where γ = 1/2 - ε - δ.

This follows by applying the Chernoff bound.

Accelerating Quantum Computing Simulations with FPGAs

With the advent of quantum computing, there has been a significant surge in both the number of developers and available tools.[7] However, the slow pace of technological advancement and the high maintenance costs associated with quantum computers have limited broader participation in this field. In response, developers have turned to simulators, such as IBM's Qiskit, to model quantum behavior without relying solely on real quantum hardware. Nevertheless, simulators, being classical computers, are constrained by computation speed. The fundamental advantage of quantum computers lies in their ability to process qubits, leveraging properties like entanglement and superposition simultaneously. By running quantum simulations on classical computers, the inherent parallelism of quantum computing is taken away. Moreover, as the number of simulated qubits increases, the simulation's speed decreases proportionally.

In a quantum circuit, the vectors are used to represent the state of the qubits and different matrices are used to represent the gate that is applied on the qubits. Since linear algebra is a major component of the quantum simulation, Field Programmable Gate Arrays (FPGAs) could be used to accelerate the simulation of quantum computing. FPGA is a kind of hardware that excels at executing operations in parallel, supports pipelining, has on-chip memory resources with low access latency, and offers the flexibility to reconfigure the hardware architecture on-the-fly which make it a well suited tool to handle matrix multiplication.

The main idea of accelerating quantum computing simulations is to offload some of the heavy computation to special hardware like FPGA in order to speed up the whole simulation process. And the bigger quantum circuits (more qubits and more gates) we simulate, the more speedup we gain from offloading to FPGA compared with software simulations on CPU. The data flow of the simulation is explained below. First, the user inputs all the information of the quantum circuit including initial state and various gates through the user interface. Then, all this information is compressed and sent to the FPGA

through some hardware communication protocols like AXI. Then, all the information is stored in the on-chip memory in the FPGA. And the simulation starts when the data is read from the memory and sent to the Matrix multiplication module. After all the calculation is done, the result will be sent back to the memory and to the CPU.

Suppose we are simulating 5-qubit circuits, then we need to store the vector that holds 32 (2^5) 16-bit values, each of which represents the square-root probability of a possible existing state. We also need to store the 32x32 matrix that represents the gate. In order to parallel this computation, we can store the 32 rows of the matrix separately and replicate 32 row_vec_mult hardware such that each row can calculate the multiplication in parallel. This will dramatically speed up the simulation with a price of more hardware and memory usage in FPGA. [8]

It has been discovered that with careful hardware design, it's possible to achieve a hardware architecture with O(n) time complexity, where 'n' denotes the number of qubits. In contrast, the runtime of Numpy approaches O(2^2^n). This finding underscores the feasibility of leveraging FPGAs to accelerate quantum computing simulations. [9]

See also

- Abstract index notation
- Angular momentum diagrams (quantum mechanics)
- Circuit complexity and BQP
- Matrix product state uses Penrose graphical notation
- Quantum register
- Spin networks
- Trace diagram

References

1. Nielsen, Michael A.; Chuang, Isaac (2010). *Quantum Computation and Quantum Information* (https://www.cambridge.org/9781107002173). Cambridge: Cambridge University Press. pp. 26–28. ISBN 978-1-10700-217-3. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
2. Colin P. Williams (2011). *Explorations in Quantum Computing*. Springer. pp. 123–200. ISBN 978-1-84628-887-6.
3. Nielsen, Michael A.; Chuang, Isaac (2010). *Quantum Computation and Quantum Information* (https://www.cambridge.org/9781107002173). Cambridge: Cambridge University Press. pp. 171–215. ISBN 978-1-10700-217-3. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
4. Ömer, Bernhard (2000-01-20). *Quantum Programming in QCL* (http://tph.tuwien.ac.at/~oemer/doc/quprog.pdf) (PDF) (Thesis). Institute for Theoretical Physics, Vienna University of Technology. pp. 37–38. Retrieved 2021-10-12.
5. Feynman, Richard P. (1986). "Quantum mechanical computers". *Foundations of Physics*. **16** (6). Springer Science and Business Media LLC: 507–531. Bibcode:1986FoPh...16..507F (https://ui.adsabs.harvard.edu/abs/1986FoPh...16..507F). doi:10.1007/bf01886518 (https://doi.org/10.1007%2Fbf01886518). ISSN 0015-9018 (https://search.worldcat.org/issn/0015-9018). S2CID 122076550 (https://api.semanticscholar.org/CorpusID:122076550).

6. "Introduction to the Quantum Circuit Model" (https://www.cs.cmu.edu/~odonnell/quantum15/QuantumComputationScribeNotesByRyanODonnellAndJohnWright.pdf) (PDF).
7. "Accelerating Quantum Simulations w/ FPGAs" (https://medium.com/@josephmeng96/accelerating-quantum-simulations-w-fpgas-84b09569ad0f). 19 August 2020.
8. "Accelerating Quantum Simulations w/ FPGAs" (https://medium.com/@josephmeng96/accelerating-quantum-simulations-w-fpgas-84b09569ad0f). 19 August 2020.
9. "Accelerating Quantum Simulations w/ FPGAs" (https://medium.com/@josephmeng96/accelerating-quantum-simulations-w-fpgas-84b09569ad0f). 19 August 2020.

- Biham, Eli; Brassard, Gilles; Kenigsberg, Dan; Mor, Tal (2004), "Quantum computing without entanglement", *Theoretical Computer Science*, **320** (1): 15–33, arXiv:quant-ph/0306182 (https://arxiv.org/abs/quant-ph/0306182), doi:10.1016/j.tcs.2004.03.041 (https://doi.org/10.1016%2Fj.tcs.2004.03.041), MR 2060181 (https://mathscinet.ams.org/mathscinet-getitem?mr=2060181), S2CID 295103 (https://api.semanticscholar.org/CorpusID:295103).
- Freedman, Michael H.; Kitaev, Alexei; Larsen, Michael J.; Wang, Zhenghan (2003), "Topological quantum computation", *Bulletin of the American Mathematical Society*, **40** (1): 31–38, arXiv:quant-ph/0101025 (https://arxiv.org/abs/quant-ph/0101025), doi:10.1090/S0273-0979-02-00964-3 (https://doi.org/10.1090%2FS0273-0979-02-00964-3), MR 1943131 (https://mathscinet.ams.org/mathscinet-getitem?mr=1943131).
- Hirvensalo, Mika (2001), *Quantum Computing*, Natural Computing Series, Berlin: Springer-Verlag, ISBN 3-540-66783-0, MR 1931238 (https://mathscinet.ams.org/mathscinet-getitem?mr=1931238).
- Kitaev, A. Yu. (1997), "Quantum computations: algorithms and error correction", *Uspekhi Mat. Nauk* (in Russian), **52** (6(318)): 53–112, Bibcode:1997RuMaS..52.1191K (https://ui.adsabs.harvard.edu/abs/1997RuMaS..52.1191K), doi:10.1070/RM1997v052n06ABEH002155 (https://doi.org/10.1070%2FRM1997v052n06ABEH002155), MR 1611329 (https://mathscinet.ams.org/mathscinet-getitem?mr=1611329), S2CID 250816585 (https://api.semanticscholar.org/CorpusID:250816585).
- Nielsen, Michael A.; Chuang, Isaac L. (2000), *Quantum Computation and Quantum Information*, Cambridge: Cambridge University Press, ISBN 0-521-63235-8, MR 1796805 (https://mathscinet.ams.org/mathscinet-getitem?mr=1796805).

External links

- Q-circuit (https://cquic.unm.edu/resources/) Archived (https://web.archive.org/web/20190323101451/https://cquic.unm.edu/resources/) 2019-03-23 at the Wayback Machine is a macro package for drawing quantum circuit diagrams in LaTeX.
- Quantum Circuit Simulator (Davy Wybiral) (https://wybiral.github.io/quantum) a browser-based quantum circuit diagram editor and simulator.
- Quantum Computing Playground (http://www.quantumplayground.net/) a browser-based quantum scripting environment.
- Quirk - Quantum Circuit Toy (http://algorithmicassertions.com/quirk) a browser-based quantum circuit diagram editor and simulator.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_circuit&oldid=1245333391"

WIKIPEDIA
The Free Encyclopedia

Quantum logic gate

In quantum computing and specifically the quantum circuit model of computation, a **quantum logic gate** (or simply **quantum gate**) is a basic quantum circuit operating on a small number of qubits. Quantum logic gates are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits.

Unlike many classical logic gates, quantum logic gates are reversible. It is possible to perform classical computing using only reversible gates. For example, the reversible Toffoli gate can implement all Boolean functions, often at the cost of having to use ancilla bits. The Toffoli gate has a direct quantum equivalent, showing that quantum circuits can perform all operations performed by classical circuits.

Quantum gates are unitary operators, and are described as unitary matrices relative to some orthonormal basis. Usually the *computational basis* is used, which unless comparing it with something, just means that for a *d*-level quantum system (such as a qubit, a quantum register, or qutrits and qudits)[1]:22–23 the orthonormal basis vectors are labeled $|0\rangle, |1\rangle, \ldots, |d-1\rangle$, or use binary notation.

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Common quantum logic gates by name (including abbreviation), circuit form(s) and the corresponding unitary matrices

History

The current notation for quantum gates was developed by many of the founders of quantum information science including Adriano Barenco, Charles Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John A. Smolin, and Harald Weinfurter,[2] building on notation introduced by Richard Feynman in 1986.[3]

Representation

Quantum logic gates are represented by unitary matrices. A gate that acts on n qubits is represented by a $2^n \times 2^n$ unitary matrix, and the set of all such gates with the group operation of matrix multiplication[a] is the unitary group U(2^n).[2] The quantum states that the gates act upon are unit vectors in 2^n complex dimensions, with the complex Euclidean norm (the 2-norm).[4]:66[5]:56,65 The basis vectors (sometimes called *eigenstates*) are the possible outcomes if the state of the qubits is measured, and a quantum state is a linear combination of these outcomes. The most common quantum gates operate on vector spaces of one or two qubits, just like the common classical logic gates operate on one or two bits.

Even though the quantum logic gates belong to continuous symmetry groups, real hardware is inexact and thus limited in precision. The application of gates typically introduces errors, and the quantum states' fidelities decrease over time. If error correction is used, the usable gates are further restricted to a finite set.[4]:ch. 10[1]:ch. 14 Later in this article, this is ignored as the focus is on the ideal quantum gates' properties.

Quantum states are typically represented by "kets", from a notation known as bra–ket.

The vector representation of a single qubit is

$$|a\rangle = v_0|0\rangle + v_1|1\rangle \to \begin{bmatrix} v_0 \\ v_1 \end{bmatrix}.$$

Here, v_0 and v_1 are the complex probability amplitudes of the qubit. These values determine the probability of measuring a 0 or a 1, when measuring the state of the qubit. See measurement below for details.

The value zero is represented by the ket $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, and the value one is represented by the ket $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

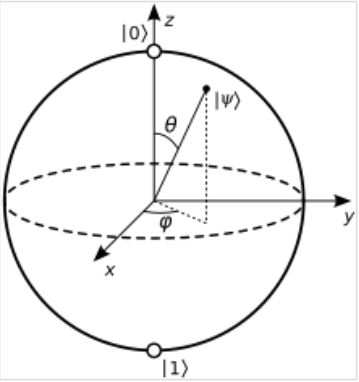
The tensor product (or Kronecker product) is used to combine quantum states. The combined state for a qubit register is the tensor product of the constituent qubits. The tensor product is denoted by the symbol $\otimes$.

The vector representation of two qubits is:[6]

$$|\psi\rangle = v_{00}|00\rangle + v_{01}|01\rangle + v_{10}|10\rangle + v_{11}|11\rangle \rightarrow \begin{bmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{bmatrix}.$$

The action of the gate on a specific quantum state is found by multiplying the vector $|\psi_1\rangle$, which represents the state by the matrix U representing the gate. The result is a new quantum state $|\psi_2\rangle$:

$$U|\psi_1\rangle = |\psi_2\rangle.$$



Single qubit states that are not entangled and lack global phase can be represented as points on the surface of the **Bloch sphere**, written as $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$. Rotations about the x, y, z axes of the Bloch sphere are represented by the rotation operator gates.

Notable examples

There exists an uncountably infinite number of gates. Some of them have been named by various authors,[2][1][4][5][7][8][9] and below follow some of those most often used in the literature.

Identity gate

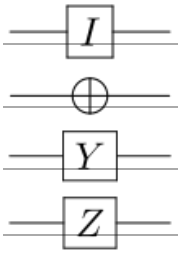
The identity gate is the identity matrix, usually written as *I*, and is defined for a single qubit as

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

where *I* is basis independent and does not modify the quantum state. The identity gate is most useful when describing mathematically the result of various gate operations or when discussing multi-qubit circuits.

Pauli gates (*X*,*Y*,*Z*)

The Pauli gates (X, Y, Z) are the three Pauli matrices $(\sigma_x, \sigma_y, \sigma_z)$ and act on a single qubit. The Pauli *X*, *Y* and *Z* equate, respectively, to a rotation around the *x*, *y* and *z* axes of the Bloch sphere by π radians.[b]



Quantum gates (from top to bottom): Identity gate, NOT gate, Pauli Y, Pauli Z

The Pauli-*X* gate is the quantum equivalent of the NOT gate for classical computers with respect to the standard basis $|0\rangle$, $|1\rangle$, which distinguishes the *z* axis on the Bloch sphere. It is sometimes called a bit-flip as it maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. Similarly, the Pauli-*Y* maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$. Pauli *Z* leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. Due to this nature, Pauli *Z* is sometimes called phase-flip.

These matrices are usually represented as

$$X = \sigma_x = \mathrm{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$
$$Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The Pauli matrices are involutory, meaning that the square of a Pauli matrix is the identity matrix.

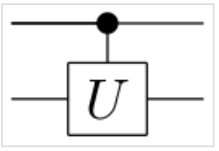
$$I^2 = X^2 = Y^2 = Z^2 = -iXYZ = I$$

The Pauli matrices also anti-commute, for example $ZX = iY = -XZ$.

The matrix exponential of a Pauli matrix σ_j is a rotation operator, often written as $e^{-i\sigma_j\theta/2}$.

Controlled gates

Controlled gates act on 2 or more qubits, where one or more qubits act as a control for some operation.[2] For example, the controlled NOT gate (or CNOT or CX) acts on 2 qubits, and performs the NOT operation on the second qubit only when the first qubit is $|1\rangle$, and otherwise leaves it unchanged. With respect to the basis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, it is represented by the Hermitian unitary matrix:



Circuit representation of controlled-*U* gate

$$\mathrm{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

The CNOT (or controlled Pauli-*X*) gate can be described as the gate that maps the basis states $|a, b\rangle \mapsto |a, a \oplus b\rangle$, where $\oplus$ is XOR.

The CNOT can be expressed in the Pauli basis as:

$$\mathrm{CNOT} = e^{i\frac{\pi}{4}(I-Z_1)(I-X_2)} = e^{-i\frac{\pi}{4}(I-Z_1)(I-X_2)}.$$

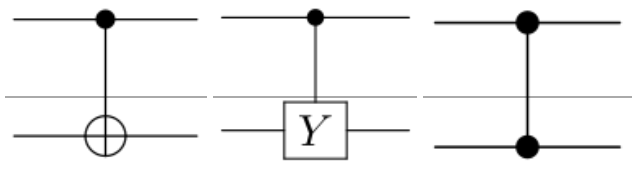
Being a Hermitian unitary operator, CNOT has the property that $e^{i\theta U} = (\cos\theta)I + (i\sin\theta)U$ and $U = e^{i\frac{\pi}{2}(I-U)} = e^{-i\frac{\pi}{2}(I-U)}$, and is involutory.

More generally if *U* is a gate that operates on a single qubit with matrix representation

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix},$$

then the *controlled-U gate* is a gate that operates on two qubits in such a way that the first qubit serves as a control. It maps the basis states as follows.

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$



Circuit diagrams of controlled Pauli gates (from left to right): CNOT (or controlled-X), controlled-Y and controlled-Z.

$$|10\rangle \mapsto |1\rangle \otimes U|0\rangle = |1\rangle \otimes (u_{00}|0\rangle + u_{10}|1\rangle)$$
$$|11\rangle \mapsto |1\rangle \otimes U|1\rangle = |1\rangle \otimes (u_{01}|0\rangle + u_{11}|1\rangle)$$

The matrix representing the controlled *U* is

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}.$$

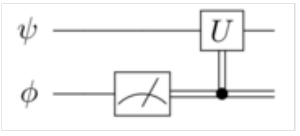
When *U* is one of the Pauli operators, *X*,*Y*, *Z*, the respective terms "controlled-*X*", "controlled-*Y*", or "controlled-*Z*" are sometimes used.[4]:177–185 Sometimes this is shortened to just C*X*, C*Y* and C*Z*.

In general, any single qubit unitary gate can be expressed as $U = e^{iH}$, where *H* is a Hermitian matrix, and then the controlled *U* is $CU = e^{i\frac{1}{2}(I-Z_1)H_2}$.

Control can be extended to gates with arbitrary number of qubits[2] and functions in programming languages.[10] Functions can be conditioned on superposition states.[11][12]

Classical control

Gates can also be controlled by classical logic. A quantum computer is controlled by a classical computer, and behaves like a coprocessor that receives instructions from the classical computer about what gates to execute on which qubits.[13]:42–43[14] Classical control is simply the inclusion, or omission, of gates in the instruction sequence for the quantum computer.[4]:26–28[1]:87–88



Example: The qubit ϕ is measured, and the result of this measurement is a Boolean value, which is consumed by the classical computer. If ϕ measures to 1, then the classical computer tells the quantum computer to apply the U gate on ψ.
In circuit diagrams, single lines are qubits, and doubled lines are bits.

Phase shift gates

The phase shift is a family of single-qubit gates that map the basis states $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\varphi}|1\rangle$. The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state. This is equivalent to tracing a horizontal circle (a line of constant latitude), or a rotation about the z-axis on the Bloch sphere by φ radians. The phase shift gate is represented by the matrix:

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

where φ is the *phase shift* with the period 2π. Some common examples are the *T* gate where $\varphi = \frac{\pi}{4}$ (historically known as the $\pi/8$ gate), the phase gate (also known as the S gate, written as *S*, though *S* is sometimes used for SWAP gates) where $\varphi = \frac{\pi}{2}$ and the Pauli-*Z* gate where $\varphi = \pi$.

The phase shift gates are related to each other as follows:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P(\pi)$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = P\left(\frac{\pi}{2}\right) = \sqrt{Z}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = P\left(\frac{\pi}{4}\right) = \sqrt{S} = \sqrt[4]{Z}$$

Note that the phase gate $P(\varphi)$ is not Hermitian (except for all $\varphi = n\pi, n \in \mathbb{Z}$). These gates are different from their Hermitian conjugates: $P^\dagger(\varphi) = P(-\varphi)$. The two adjoint (or conjugate transpose) gates $S^\dagger$ and $T^\dagger$ are sometimes included in instruction sets.[15][16]

Hadamard gate

The Hadamard or Walsh-Hadamard gate, named after Jacques Hadamard (French: [adamaʁ]) and Joseph L. Walsh, acts on a single qubit. It maps the basis states $|0\rangle \mapsto \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle \mapsto \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ (it creates an equal superposition state if given a computational basis state). The two states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ are sometimes written $|+\rangle$ and $|-\rangle$ respectively. The Hadamard

gate performs a rotation of π about the axis $(\hat{x}+\hat{z})/\sqrt{2}$ at the Bloch sphere, and is therefore involutory. It is represented by the Hadamard matrix:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}.$$



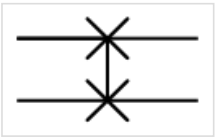
Circuit representation of Hadamard gate

If the Hermitian (so $H^\dagger = H^{-1} = H$) Hadamard gate is used to perform a change of basis, it flips $\hat{x}$ and $\hat{z}$. For example, $HZH = X$ and $H\sqrt{X}\,H = \sqrt{Z} = S$.

Swap gate

The swap gate swaps two qubits. With respect to the basis $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, it is represented by the matrix

$$\mathrm{SWAP} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}.$$

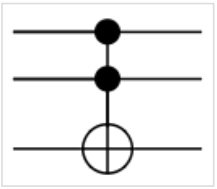

Circuit representation of SWAP gate

The swap gate can be decomposed into summation form:

$$\mathrm{SWAP} = \frac{I\otimes I + X\otimes X + Y\otimes Y + Z\otimes Z}{2}$$

Toffoli (CCNOT) gate

The Toffoli gate, named after Tommaso Toffoli and also called the CCNOT gate or Deutsch gate $D(\pi/2)$, is a 3-bit gate that is universal for classical computation but not for quantum computation. The quantum Toffoli gate is the same gate, defined for 3 qubits. If we limit ourselves to only accepting input qubits that are $|0\rangle$ and $|1\rangle$, then if the first two bits are in the state $|1\rangle$ it applies a Pauli-*X* (or NOT) on the third bit, else it does nothing. It is an example of a CC-U (controlled-controlled Unitary) gate. Since it is the quantum analog of a classical gate, it is completely specified by its truth table. The Toffoli gate is universal when combined with the single qubit Hadamard gate.[17]


Circuit representation of Toffoli gate

Truth table

INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Matrix form

$$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$$

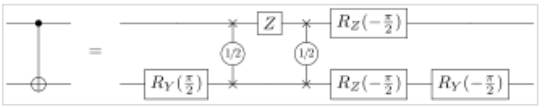
The Toffoli gate is related to the classical AND ($\wedge$) and XOR ($\oplus$) operations as it performs the mapping $|a,b,c\rangle \mapsto |a,b,c\oplus(a\wedge b)\rangle$ on states in the computational basis.

The Toffoli gate can be expressed using Pauli matrices as

$$\mathrm{Toff} = e^{i\frac{\pi}{8}(I-Z_1)(I-Z_2)(I-X_3)} = e^{-i\frac{\pi}{8}(I-Z_1)(I-Z_2)(I-X_3)}.$$

Universal quantum gates

A set of **universal quantum gates** is any set of gates to which any operation possible on a quantum computer can be reduced, that is, any other unitary operation can be expressed as a finite sequence of gates from the set. Technically, this is impossible with anything less than an uncountable set of gates since the number of possible quantum gates is uncountable, whereas the number of finite sequences from a finite set is countable. To solve this problem, we only require that any quantum operation can be approximated by a sequence of gates from this finite set. Moreover, for unitaries on a constant number of qubits, the Solovay–Kitaev theorem guarantees that this can be done efficiently. Checking if a set of quantum gates is universal can be done using group theory methods[18] and/or relation to (approximate) unitary t-designs[19]



Both CNOT and $\sqrt{\text{SWAP}}$ are universal two-qubit gates and can be transformed into each other.

Some universal quantum gate sets include:

- The rotation operators $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$, the phase shift gate $P(\varphi)$[c] and CNOT are commonly used to form a universal quantum gate set.[20][d]
- The Clifford set {CNOT, H, S} + T gate. The Clifford set alone is not a universal quantum gate set, as it can be efficiently simulated classically according to the Gottesman–Knill theorem.
- The Toffoli gate + Hadamard gate.[17] The Toffoli gate alone forms a set of universal gates for reversible Boolean algebraic logic circuits, which encompasses all classical computation.

Deutsch gate

A single-gate set of universal quantum gates can also be formulated using the parametrized three-qubit Deutsch gate $D(\theta)$,[21] named after physicist David Deutsch. It is a general case of *CC-U*, or *controlled-controlled-unitary* gate, and is defined as

$$|a,b,c\rangle \mapsto \begin{cases} i\cos(\theta)|a,b,c\rangle + \sin(\theta)|a,b,1-c\rangle & \text{for } a=b=1, \\ |a,b,c\rangle & \text{otherwise.} \end{cases}$$

Unfortunately, a working Deutsch gate has remained out of reach, due to lack of a protocol. There are some proposals to realize a Deutsch gate with dipole–dipole interaction in neutral atoms.[22]

A universal logic gate for reversible classical computing, the Toffoli gate, is reducible to the Deutsch gate $D(\pi/2)$, thus showing that all reversible classical logic operations can be performed on a universal quantum computer.

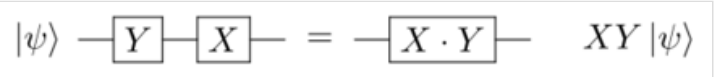
There also exist single two-qubit gates sufficient for universality. In 1996, Adriano Barenco showed that the Deutsch gate can be decomposed using only a single two-qubit gate (Barenco gate), but it is hard to realize experimentally.[1]:93 This feature is exclusive to quantum circuits, as there is no classical two-bit gate that is both reversible and universal.[1]:93 Universal two-qubit gates could be implemented to improve classical reversible circuits in fast low-power microprocessors.[1]:93

Circuit composition

Serially wired gates

Assume that we have two gates A and B that both act on n qubits. When B is put after A in a series circuit, then the effect of the two gates can be described as a single gate C.

$$C = B \cdot A$$



Two gates Y and X in series. The order in which they appear on the wire is reversed when multiplying them together.

where $\cdot$ is matrix multiplication. The resulting gate C will have the same dimensions as A and B. The order in which the gates would appear in a circuit diagram is reversed when multiplying them together.[4]:17–18,22–23,62–64[5]:147–169

For example, putting the Pauli X gate after the Pauli Y gate, both of which act on a single qubit, can be described as a single combined gate C:

$$C = X \cdot Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = iZ$$

The product symbol (·) is often omitted.

Exponents of quantum gates

All real exponents of unitary matrices are also unitary matrices, and all quantum gates are unitary matrices.

Positive integer exponents are equivalent to sequences of serially wired gates (e.g. $X^3 = X \cdot X \cdot X$), and the real exponents is a generalization of the series circuit. For example, X^π and $\sqrt{X} = X^{1/2}$ are both valid quantum gates.

$U^0 = I$ for any unitary matrix U. The identity matrix (I) behaves like a NOP[23][24] and can be represented as bare wire in quantum circuits, or not shown at all.

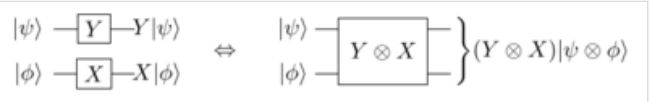
All gates are unitary matrices, so that $U^\dagger U = UU^\dagger = I$ and $U^\dagger = U^{-1}$, where † is the conjugate transpose. This means that negative exponents of gates are unitary inverses of their positively exponentiated counterparts: $U^{-n} = (U^n)^\dagger$. For example, some negative exponents of the phase shift gates are $T^{-1} = T^\dagger$ and $T^{-2} = (T^2)^\dagger = S^\dagger$.

Note that for a Hermitian matrix $H^\dagger = H$, and because of unitarity, $HH^\dagger = I$, so $H^2 = I$ for all Hermitian gates. They are involutory. Examples of Hermitian gates are the Pauli gates, Hadamard, CNOT, SWAP and Toffoli. Each Hermitian unitary matrix H has the property that $e^{i\theta H} = (\cos\theta)I + (i\sin\theta)H$ where $H = e^{i\frac{\pi}{2}(I-H)} = e^{-i\frac{\pi}{2}(I-H)}$.

Parallel gates

The tensor product (or Kronecker product) of two quantum gates is the gate that is equal to the two gates in parallel.[4]:71–75[5]:148

If we, as in the picture, combine the Pauli-*Y* gate with the Pauli-*X* gate in parallel, then this can be written as:



Two gates Y and X in parallel is equivalent to the gate $Y \otimes X$.

$$C = Y \otimes X = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & -i\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \\ i\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & 0\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ i & 0 & 0 & 0 \end{bmatrix}$$

Both the Pauli-*X* and the Pauli-*Y* gate act on a single qubit. The resulting gate C act on two qubits.

Sometimes the tensor product symbol is omitted, and indexes are used for the operators instead.[25]

Hadamard transform

The gate $H_2 = H \otimes H$ is the Hadamard gate (H) applied in parallel on 2 qubits. It can be written as:

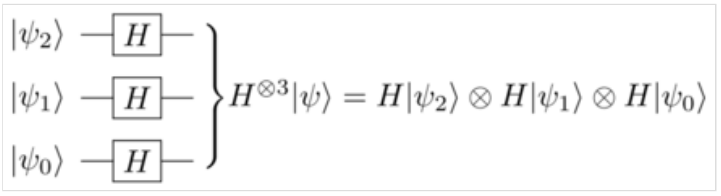
$$H_2 = H \otimes H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

This "two-qubit parallel Hadamard gate" will, when applied to, for example, the two-qubit zero-vector ($|00\rangle$), create a quantum state that has equal probability of being observed in any of its four possible outcomes; $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. We can write this operation as:

$$H_2|00\rangle = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Here the amplitude for each measurable state is $1/2$. The probability to observe any state is the square of the absolute value of the measurable states amplitude, which in the above example means that there is one in four that we observe any one of the individual four cases. See measurement for details.

$\boldsymbol{H_2}$ performs the Hadamard transform on two qubits. Similarly the gate $\underbrace{\boldsymbol{H} \otimes \boldsymbol{H} \otimes \cdots \otimes \boldsymbol{H}}_{n \text{ times}} = \bigotimes_{1}^{n} \boldsymbol{H} = \boldsymbol{H}^{\otimes n} = \boldsymbol{H_n}$ performs a Hadamard transform on a register of $\boldsymbol{n}$ qubits.



Example: The Hadamard transform on a 3-qubit register $|\psi\rangle$.

When applied to a register of $\boldsymbol{n}$ qubits all initialized to $|\mathbf{0}\rangle$, the Hadamard transform puts the quantum register into a superposition with equal probability of being measured in any of its $\boldsymbol{2^n}$ possible states:

$$\bigotimes_{0}^{n-1}(H|0\rangle) = \frac{1}{\sqrt{2^n}}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix} = \frac{1}{\sqrt{2^n}}\Big(|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle\Big) = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$$

This state is a *uniform superposition* and it is generated as the first step in some search algorithms, for example in amplitude amplification and phase estimation.

Measuring this state results in a random number between $|0\rangle$ and $|2^n - 1\rangle$.[e] How random the number is depends on the fidelity of the logic gates. If not measured, it is a quantum state with equal probability amplitude $\frac{1}{\sqrt{2^n}}$ for each of its possible states.

The Hadamard transform acts on a register $|\psi\rangle$ with $\boldsymbol{n}$ qubits such that $|\psi\rangle = \bigotimes_{i=0}^{n-1}|\psi_i\rangle$ as follows:

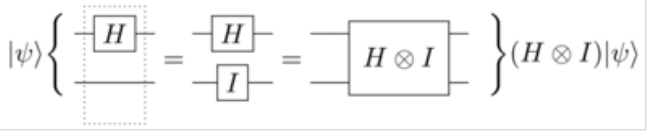
$$\bigotimes_{0}^{n-1} H|\psi\rangle = \bigotimes_{i=0}^{n-1}\frac{|0\rangle + (-1)^{\psi_i}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^n}}\bigotimes_{i=0}^{n-1}\Big(|0\rangle + (-1)^{\psi_i}|1\rangle\Big) = H|\psi_0\rangle \otimes H|\psi_1\rangle \otimes \cdots \otimes H|\psi_{n-1}\rangle$$

Application on entangled states

If two or more qubits are viewed as a single quantum state, this combined state is equal to the tensor product of the constituent qubits. Any state that can be written as a tensor product from the constituent subsystems are called *separable states*. On the other hand, an *entangled state* is any state that cannot be tensor-factorized, or in other words: *An entangled state can not be written as a tensor product of its constituent qubits states.* Special care must be taken when applying gates to constituent qubits that make up entangled states.

If we have a set of *N* qubits that are entangled and wish to apply a quantum gate on *M* < *N* qubits in the set, we will have to extend the gate to take *N* qubits. This application can be done by combining the gate with an identity matrix such that their tensor product becomes a gate that act on *N* qubits. The identity matrix ($\boldsymbol{I}$) is a representation of the gate that maps every state to itself (i.e., does nothing at all). In a circuit diagram the identity gate or matrix will often appear as just a bare wire.

For example, the Hadamard gate ($\boldsymbol{H}$) acts on a single qubit, but if we feed it the first of the two qubits that constitute the entangled Bell state $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, we cannot write that operation easily. We need to extend the Hadamard gate $\boldsymbol{H}$ with the identity gate $\boldsymbol{I}$ so that we can act on quantum states that span *two* qubits:



The example given in the text. The Hadamard gate $\boldsymbol{H}$ only act on 1 qubit, but $|\psi\rangle$ is an entangled quantum state that spans 2 qubits. In our example, $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

$$\boldsymbol{K} = \boldsymbol{H} \otimes \boldsymbol{I} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 1\\1 & 0 & -1 & 0\\0 & 1 & 0 & -1\end{bmatrix}$$

The gate $\boldsymbol{K}$ can now be applied to any two-qubit state, entangled or otherwise. The gate $\boldsymbol{K}$ will leave the second qubit untouched and apply the Hadamard transform to the first qubit. If applied to the Bell state in our example, we may write that as:

$$K\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1\\1\\1\\-1\end{bmatrix} = \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2}$$

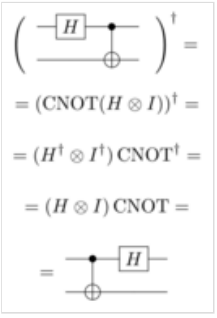
Computational complexity and the tensor product

The time complexity for multiplying two $n \times n$-matrices is at least $\Omega(n^2 \log n)$,[26] if using a classical machine. Because the size of a gate that operates on q qubits is $2^q \times 2^q$ it means that the time for simulating a step in a quantum circuit (by means of multiplying the gates) that operates on generic entangled states is $\Omega(2^{q^2} \log(2^q))$. For this reason it is believed to be intractable to simulate large entangled quantum systems using classical computers. Subsets of the gates, such as the Clifford gates, or the trivial case of circuits that only implement classical Boolean functions (e.g. combinations of X, CNOT, Toffoli), can however be efficiently simulated on classical computers.

The state vector of a quantum register with n qubits is 2^n complex entries. Storing the probability amplitudes as a list of floating point values is not tractable for large n.

Unitary inversion of gates

Because all quantum logical gates are reversible, any composition of multiple gates is also reversible. All products and tensor products (i.e. series and parallel combinations) of unitary matrices are also unitary matrices. This means that it is possible to construct an inverse of all algorithms and functions, as long as they contain only gates.



Example: The unitary inverse of the Hadamard-CNOT product. The three gates $\boldsymbol{H}$, $\boldsymbol{I}$ and $\mathbf{CNOT}$ are their own unitary inverses.

Initialization, measurement, I/O and spontaneous decoherence are side effects in quantum computers. Gates however are purely functional and bijective.

If U is a unitary matrix, then $U^\dagger U = UU^\dagger = I$ and $U^\dagger = U^{-1}$. The dagger (†) denotes the conjugate transpose. It is also called the Hermitian adjoint.

If a function F is a product of m gates, $F = A_1 \cdot A_2 \cdot \cdots \cdot A_m$, the unitary inverse of the function $F^\dagger$ can be constructed:

Because $(UV)^\dagger = V^\dagger U^\dagger$ we have, after repeated application on itself

$$F^\dagger = \left(\prod_{i=1}^{m} A_i\right)^\dagger = \prod_{i=m}^{1} A_i^\dagger = A_m^\dagger \cdot \cdots \cdot A_2^\dagger \cdot A_1^\dagger$$

Similarly if the function G consists of two gates A and B in parallel, then $G = A \otimes B$ and $G^\dagger = (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

Gates that are their own unitary inverses are called Hermitian or self-adjoint operators. Some elementary gates such as the Hadamard (*H*) and the Pauli gates (*I*, *X*, *Y*, *Z*) are Hermitian operators, while others like the phase shift (*S*, *T*, *P*, CPhase) gates generally are not.

For example, an algorithm for addition can be used for subtraction, if it is being "run in reverse", as its unitary inverse. The inverse quantum Fourier transform is the unitary inverse. Unitary inverses can also be used for uncomputation. Programming languages for quantum computers, such as Microsoft's Q#,[10] Bernhard Ömer's QCL,[13]:61 and IBM's Qiskit,[27] contain function inversion as programming concepts.

Measurement

Measurement (sometimes called *observation*) is irreversible and therefore not a quantum gate, because it assigns the observed quantum state to a single value. Measurement takes a quantum state and projects it to one of the basis vectors, with a likelihood equal to the square of the vector's length (in the 2-norm[4]:66[5]:56,65) along that basis vector.[1]:15–17[28][29][30] This is known as the Born rule and appears[e] as a stochastic non-reversible operation as it probabilistically sets the quantum state equal to the basis vector that represents the measured state. At the instant of measurement, the state is said to "collapse" to the definite single value that was measured. Why and how, or even if[31][32] the quantum state collapses at measurement, is called the measurement problem.

The probability of measuring a value with probability amplitude ϕ is $1 \geq |\phi|^2 \geq 0$, where $|\cdot|$ is the modulus.

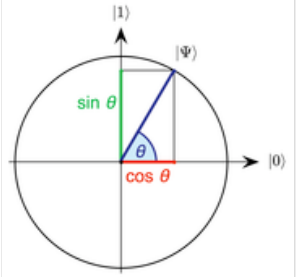


Circuit representation of measurement. The two lines on the right hand side represent a classical bit, and the single line on the left hand side represents a qubit.

Measuring a single qubit, whose quantum state is represented by the vector $a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, will result in $|0\rangle$ with probability $|a|^2$, and in $|1\rangle$ with probability $|b|^2$.

For example, measuring a qubit with the quantum state $\frac{|0\rangle - i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}$ will yield with equal probability either $|0\rangle$ or $|1\rangle$.

A quantum state $|\Psi\rangle$ that spans n qubits can be written as a vector in 2^n complex dimensions: $|\Psi\rangle \in \mathbb{C}^{2^n}$. This is because the tensor product of n qubits is a vector in 2^n dimensions. This way, a register of n qubits can be measured to 2^n distinct states, similar to how a register of n classical bits can hold 2^n distinct states. Unlike with the bits of classical computers, quantum states can have non-zero probability amplitudes in multiple measurable values simultaneously. This is called *superposition*.



For a single qubit, we have a unit sphere in $\mathbb{C}^2$ with the quantum state $a|0\rangle + b|1\rangle$ such that $|a|^2 + |b|^2 = 1$. The state can be re-written as $|\cos\theta|^2 + |\sin\theta|^2 = 1$, or $|a|^2 = \cos^2\theta$ and $|b|^2 = \sin^2\theta$.
Note: $|a|^2$ is the probability of measuring $|0\rangle$ and $|b|^2$ is the probability of measuring $|1\rangle$.

The sum of all probabilities for all outcomes must always be equal to 1.[f] Another way to say this is that the Pythagorean theorem generalized to $\mathbb{C}^{2^n}$ has that all quantum states $|\Psi\rangle$ with n qubits must satisfy $1 = \sum_{x=0}^{2^n-1} |a_x|^2$,[g] where a_x is the probability amplitude for measurable state $|x\rangle$. A geometric interpretation of this is that the possible value-space of a quantum state $|\Psi\rangle$ with n qubits is the surface of the unit sphere in $\mathbb{C}^{2^n}$ and that the unitary transforms (i.e. quantum logic gates) applied to it are rotations on the sphere. The rotations that the gates perform form the symmetry group U(2^n). Measurement is then a probabilistic projection of the points at the surface of this complex sphere onto the basis vectors that span the space (and labels the outcomes).

In many cases the space is represented as a Hilbert space $\mathcal{H}$ rather than some specific 2^n-dimensional complex space. The number of dimensions (defined by the basis vectors, and thus also the possible outcomes from measurement) is then often implied by the operands, for example as the required state space for solving a problem. In Grover's algorithm, Grover named this generic basis vector set *"the database"*.

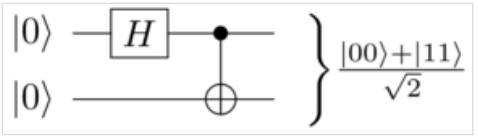
The selection of basis vectors against which to measure a quantum state will influence the outcome of the measurement.[1]:30–35[4]:22,84–85,185–188[33] See change of basis and Von Neumann entropy for details. In this article, we always use the *computational basis*, which means that we have labeled the 2^n basis vectors of an n-qubit register $|0\rangle, |1\rangle, |2\rangle, \cdots, |2^n - 1\rangle$, or use the binary representation $|0_{10}\rangle = |0\ldots00_2\rangle, |1_{10}\rangle = |0\ldots01_2\rangle, |2_{10}\rangle = |0\ldots10_2\rangle, \cdots, |2^n - 1\rangle = |111\ldots1_2\rangle$.

In quantum mechanics, the basis vectors constitute an orthonormal basis.

An example of usage of an alternative measurement basis is in the BB84 cipher.

The effect of measurement on entangled states

If two quantum states (i.e. qubits, or registers) are entangled (meaning that their combined state cannot be expressed as a tensor product), measurement of one register affects or reveals the state of the other register by partially or entirely collapsing its state too. This effect can be used for computation, and is used in many algorithms.



The Hadamard-CNOT gate, which when given the input $|00\rangle$ produces a Bell state

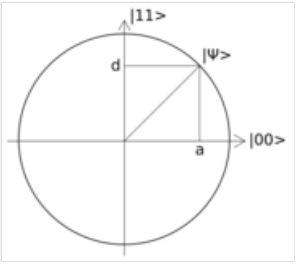
The Hadamard-CNOT combination acts on the zero-state as follows:

$$\mathrm{CNOT}(H \otimes I)|00\rangle = \left(\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right)\right)\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

This resulting state is the Bell state $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$. It cannot be described as a tensor product of two qubits. There is no solution for

$$\begin{bmatrix}x\\y\end{bmatrix} \otimes \begin{bmatrix}w\\z\end{bmatrix} = \begin{bmatrix}xw\\xz\\yw\\yz\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix},$$

because for example *w* needs to be both non-zero and zero in the case of *xw* and *yw*.



The Bell state in the text is $|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ where $a = d = \frac{1}{\sqrt{2}}$ and $b = c = 0$. Therefore, it can be described by the plane spanned by the basis vectors $|00\rangle$ and $|11\rangle$, as in the picture. The unit sphere (in $\mathbb{C}^4$) that represent the possible value-space of the 2-qubit system intersects the plane and $|\Psi\rangle$ lies on the unit spheres surface. Because $|a|^2 = |d|^2 = 1/2$, there is equal probability of measuring this state to $|00\rangle$ or $|11\rangle$, and because $b = c = 0$ there is zero probability of measuring it to $|01\rangle$ or $|10\rangle$.

The quantum state *spans* the two qubits. This is called *entanglement*. Measuring one of the two qubits that make up this Bell state will result in that the other qubit logically must have the same value, both must be the same: Either it will be found in the state $|00\rangle$, or in the state $|11\rangle$. If we measure one of the qubits to be for example $|1\rangle$, then the other qubit must also be $|1\rangle$, because their combined state *became* $|11\rangle$. Measurement of one of the qubits collapses the entire quantum state, that span the two qubits.

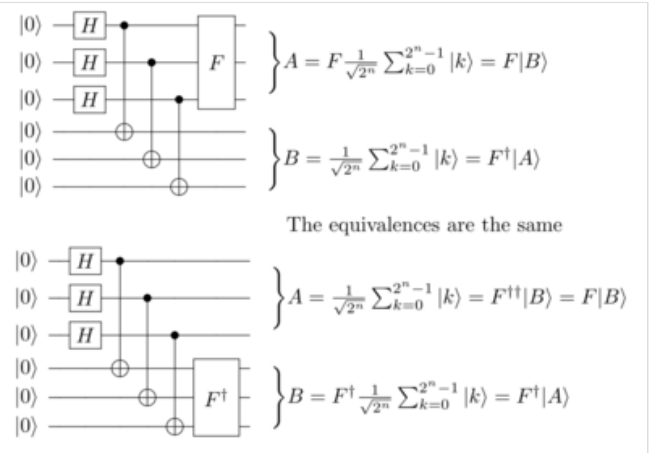
The GHZ state is a similar entangled quantum state that spans three or more qubits.

This type of value-assignment occurs *instantaneously over any distance* and this has as of 2018 been experimentally verified by QUESS for distances of up to 1200 kilometers.[34][35][36] That the phenomena appears to happen instantaneously as opposed to the time it would take to traverse the distance separating the qubits at the speed of light is called the EPR paradox, and it is an open question in physics how to resolve this. Originally it was solved by giving up the assumption of local realism, but other interpretations have also emerged. For more information see the Bell test experiments. The no-communication theorem proves that this phenomenon cannot be used for faster-than-light communication of classical information.

Measurement on registers with pairwise entangled qubits

Take a register A with n qubits all initialized to $|0\rangle$, and feed it through a parallel Hadamard gate $H^{\otimes n}$. Register A will then enter the state $\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle$ that have equal probability of when measured to be in any of its 2^n possible states; $|0\rangle$ to $|2^n-1\rangle$. Take a second register B, also with n qubits initialized to $|0\rangle$ and pairwise CNOT its qubits with the qubits in register A, such that for each p the qubits A_p and B_p forms the state $|A_pB_p\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$.

If we now measure the qubits in register A, then register B will be found to contain the same value as A. If we however instead apply a quantum logic gate F on A and then measure, then $|A\rangle = F|B\rangle \iff F^\dagger|A\rangle = |B\rangle$, where $F^\dagger$ is the unitary inverse of F.



The effect of a unitary transform F on a register A that is in a superposition of 2^n states and pairwise entangled with the register B. Here, *n* is 3 (each register has 3 qubits).

Because of how unitary inverses of gates act, $F^\dagger|A\rangle = F^{-1}(|A\rangle) = |B\rangle$. For example, say $F(x) = x + 3 \pmod{2^n}$, then $|B\rangle = |A - 3 \pmod{2^n}\rangle$.

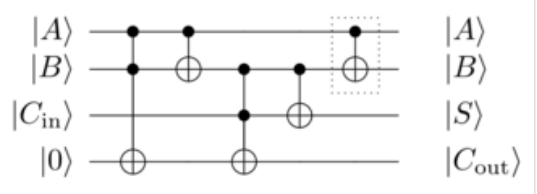
The equality will hold no matter in which order measurement is performed (on the registers A or B), assuming that F has run to completion. Measurement can even be randomly and concurrently interleaved qubit by qubit, since the measurements assignment of one qubit will limit the possible value-space from the other entangled qubits.

Even though the equalities holds, the probabilities for measuring the possible outcomes may change as a result of applying F, as may be the intent in a quantum search algorithm.

This effect of value-sharing via entanglement is used in Shor's algorithm, phase estimation and in quantum counting. Using the Fourier transform to amplify the probability amplitudes of the solution states for some problem is a generic method known as "Fourier fishing".[37]

Logic function synthesis

Functions and routines that only use gates can themselves be described as matrices, just like the smaller gates. The matrix that represents a quantum function acting on q qubits has size $2^q \times 2^q$. For example, a function that acts on a "qubyte" (a register of 8 qubits) would be represented by a matrix with $2^8 \times 2^8 = 256 \times 256$ elements.



A quantum full adder, given by Feynman in 1986.[3] It consists of only Toffoli and CNOT gates. The gate that is surrounded by the dotted square in this picture can be omitted if uncomputation to restore the *B output* is not required.

Unitary transformations that are not in the set of gates natively available at the quantum computer (the primitive gates) can be synthesised, or approximated, by combining the available primitive gates in a circuit. One way to do this is to factor the matrix that encodes the unitary transformation into a product of tensor products (i.e. series and parallel circuits) of the available primitive gates. The group $U(2^q)$ is the symmetry group for the gates that act on q qubits.[2] Factorization is then the problem of finding a path in $U(2^q)$ from the generating set of primitive gates. The Solovay–Kitaev theorem shows that given a sufficient set of primitive gates, there exist an efficient approximate for any gate. For the general case with a large number of qubits this direct approach to circuit synthesis is intractable.[38][39] This puts a limit on how large functions can be brute-force factorized into primitive quantum gates. Typically quantum programs are instead built using relatively small and simple quantum functions, similar to normal classical programming.

Because of the gates unitary nature, all functions must be reversible and always be bijective mappings of input to output. There must always exist a function F^{-1} such that $F^{-1}(F(|\psi\rangle)) = |\psi\rangle$. Functions that are not invertible can be made invertible by adding ancilla qubits to the input or the output, or both. After the function has run to completion, the ancilla qubits can then either be uncomputed or left untouched. Measuring or otherwise collapsing the quantum state of an ancilla qubit (e.g. by re-initializing the value of it, or by its spontaneous decoherence) that have not been uncomputed may result in errors,[40][41] as their state may be entangled with the qubits that are still being used in computations.

Logically irreversible operations, for example addition modulo 2^n of two n-qubit registers *a* and *b*, $F(a, b) = a + b \pmod{2^n}$,[h] can be made logically reversible by adding information to the output, so that the input can be computed from the output (i.e. there exists a function F^{-1}). In our example, this can be done by passing on one of the input registers to the output: $F(|a\rangle \otimes |b\rangle) = |a + b \pmod{2^n}\rangle \otimes |a\rangle$. The output can then be used to compute the input (i.e. given the output $a + b$ and a, we can easily find the input; a is given and $(a + b) - a = b$) and the function is made bijective.

All Boolean algebraic expressions can be encoded as unitary transforms (quantum logic gates), for example by using combinations of the Pauli-X, CNOT and Toffoli gates. These gates are functionally complete in the Boolean logic domain.

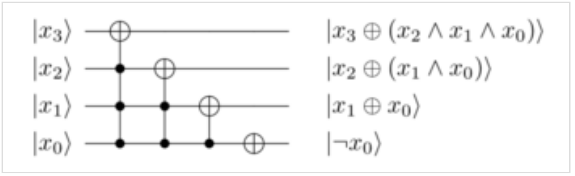
There are many unitary transforms available in the libraries of Q#, QCL, Qiskit, and other quantum programming languages. It also appears in the literature.[42][43]

For example, $\mathbf{inc}(|x\rangle) = |x + 1 \pmod{2^{x_{\text{length}}}}\rangle$, where x_{length} is the number of qubits that constitutes the register x, is implemented as the following in QCL:[44][13][12]

```
cond qufunct inc(qureg x) { // increment register
  int i;
  for i = #x-1 to 0 step -1 {
    CNot(x[i], x[0::i]);     // apply controlled-not from
  }                          // MSB to LSB
}
```

In QCL, decrement is done by "undoing" increment. The prefix `!` is used to instead run the unitary inverse of the function. `!inc(x)` is the inverse of `inc(x)` and instead performs the operation $\mathbf{inc}^\dagger|x\rangle = \mathbf{inc}^{-1}(|x\rangle) = |x - 1 \pmod{2^{x_{\text{length}}}}\rangle$. The `cond` keyword means that the function can be conditional.[11]

In the model of computation used in this article (the quantum circuit model), a classic computer generates the gate composition for the quantum computer, and the quantum computer behaves as a coprocessor that receives instructions from the classical computer about which primitive gates to apply to which qubits.[13]:36–43[14] Measurement of quantum registers results in binary values that the classical computer can use in its computations. Quantum algorithms often contain both a classical and a quantum part. Unmeasured I/O (sending qubits to remote computers without collapsing their quantum states) can be used to create networks of quantum computers. Entanglement swapping can then be used to realize distributed algorithms with quantum computers that are not directly connected. Examples of distributed algorithms that only require the use of a handful of quantum logic gates are superdense coding, the quantum Byzantine agreement and the BB84 cipherkey exchange protocol.



The generated circuit, when $x_{\text{length}} = 4$. The symbols $\oplus$, $\wedge$ and $\neg$ denotes XOR, AND and NOT respectively, and comes from the Boolean representation of Pauli-*X* with zero or more control qubits when applied to states that are in the computational basis.

See also

- Adiabatic quantum computation
- BQP
- Cellular automaton
- Cloud-based quantum computing
- Counterfactual definiteness
- Counterfactual quantum computation
- Landauer's principle
- Logical connective
- One-way quantum computer
- Quantum algorithm
- Quantum cellular automaton
- Quantum channel
- Quantum finite automaton
- Quantum logic
- Quantum memory
- Quantum network
- Quantum Zeno effect
- Reversible computing
- Unitary transformation (quantum mechanics)

Notes

a. Matrix multiplication of quantum gates is defined as series circuits.

b. Note, here a full rotation about the Bloch sphere is 2π radians, as opposed to the rotation operator gates where a full turn is 4π.

c. Either the P or Ph gate can be used, as $R_z(\delta)\,\mathrm{Ph}(\delta/2) = P(\delta)$[2]:11[1]:76–83

d. This set generates every possible unitary gate exactly. However as the global phase is irrelevant in the measurement output, universal quantum subsets can be constructed e.g. the set containing $R_y(\theta)$,$R_z(\theta)$ and CNOT only spans all unitaries with determinant ±1 but it is sufficient for quantum computation.

e. If this actually is a stochastic effect depends on which interpretation of quantum mechanics that is correct (and if any interpretation can be correct). For example, De Broglie–Bohm theory and the many-worlds interpretation asserts determinism. (In the many-worlds interpretation, a quantum computer is a machine that runs programs (quantum circuits) that selects a reality where the probability of it having the solution states of a problem is large. That is, the machine more often than not ends up in a reality where it gives the correct answer. Because *all* outcomes are realized in separate universes according to the many-worlds interpretation, the total outcome is deterministic. This *interpretation* does however not change the mechanics by which the machine operates.)

f. See Probability axioms § Second axiom

g. The hypotenuse has length 1 because the probabilities sum to 1, so the quantum state vector is a unit vector.

h. The input is $2n$ qubits, but the output is just n qubits. Information erasure is not a reversible (or unitary) operation, and therefore not allowed. See also Landauer's principle.

References

1. Colin P. Williams (2011). *Explorations in Quantum Computing*. Springer. ISBN 978-1-84628-887-6.

2. Barenco, Adriano; Bennett, Charles H.; Cleve, Richard; DiVincenzo, David P.; Margolus, Norman; Shor, Peter; Sleator, Tycho; Smolin, John A.; Weinfurter, Harald (1995-11-01). "Elementary gates for quantum computation". *Physical Review A*. **52** (5). American Physical Society (APS): 3457–3467. arXiv:quant-ph/9503016 (https://arxiv.org/abs/quant-ph/9503016). Bibcode:1995PhRvA..52.3457B (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.3457B). doi:10.1103/physreva.52.3457 (https://doi.org/10.1103%2Fphysreva.52.3457). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). PMID 9912645 (https://pubmed.ncbi.nlm.nih.gov/9912645). S2CID 8764584 (https://api.semanticscholar.org/CorpusID:8764584).
3. Feynman, Richard P. (1986). "Quantum mechanical computers". *Foundations of Physics*. **16** (6). Springer Science and Business Media LLC: 507–531. Bibcode:1986FoPh...16..507F (https://ui.adsabs.harvard.edu/abs/1986FoPh...16..507F). doi:10.1007/bf01886518 (https://doi.org/10.1007%2Fbf01886518). ISSN 0015-9018 (https://search.worldcat.org/issn/0015-9018). S2CID 122076550 (https://api.semanticscholar.org/CorpusID:122076550).
4. Nielsen, Michael A.; Chuang, Isaac (2010). *Quantum Computation and Quantum Information* (https://www.cambridge.org/9781107002173). Cambridge: Cambridge University Press. ISBN 978-1-10700-217-3. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
5. Yanofsky, Noson S.; Mannucci, Mirco (2013). *Quantum computing for computer scientists*. Cambridge University Press. ISBN 978-0-521-87996-5.
6. Preskill, John (2021-06-06). "Quantum computing 40 years later". pp. 10–15. arXiv:2106.10522 (https://arxiv.org/abs/2106.10522) [quant-ph (https://arxiv.org/archive/quant-ph)].
7. "Circuit Library" (https://qiskit.org/documentation/apidoc/circuit_library.html). IBM (Qiskit).
8. "cQASM: Qubit gate operations" (https://www.quantum-inspire.com/kbase/cqasm-qubit-gate-operations/). QuTech.
9. "Microsoft.Quantum.Intrinsic namespace" (https://docs.microsoft.com/en-us/qsharp/api/qsharp/microsoft.quantum.intrinsic). Microsoft (Q#). 28 July 2023.
10. Operations and Functions (Q# documentation) (https://docs.microsoft.com/en-us/quantum/user-guide/using-qsharp/operations-functions?view=qsharp-preview#controlled-and-adjoint-operations)
11. Ömer, Bernhard (2 September 2009). "Structured Quantum Programming" (https://web.archive.org/web/20220327170025/tph.tuwien.ac.at/~oemer/doc/structquprog.pdf) (PDF). Institute for Theoretical Physics, Vienna University of Technology. pp. 72, 92–107. Archived from the original (http://tph.tuwien.ac.at/~oemer/doc/structquprog.pdf) (PDF) on March 27, 2022.
12. Ömer, Bernhard (29 Apr 2003). "Classical Concepts in Quantum Programming". *International Journal of Theoretical Physics*. **44** (7): 943–955. arXiv:quant-ph/0211100 (https://arxiv.org/abs/quant-ph/0211100). doi:10.1007/s10773-005-7071-x (https://doi.org/10.1007%2Fs10773-005-7071-x). S2CID 119373370 (https://api.semanticscholar.org/CorpusID:119373370).
13. Ömer, Bernhard (2000-01-20). *Quantum Programming in QCL* (https://web.archive.org/web/20220601141903/http://tph.tuwien.ac.at/~oemer/doc/quprog.pdf) (PDF) (Thesis). Institute for Theoretical Physics, Vienna University of Technology. Archived from the original (http://tph.tuwien.ac.at/~oemer/doc/quprog.pdf) (PDF) on June 1, 2022. Retrieved 2021-05-24.
14. Pauka SJ, Das W, Kalra R, Moini A, Yang Y, Trainer M, Bousquet A, Cantaloube C, Dick N, Gardner GC, Manfra MJ, Reilly DJ (2021). "A cryogenic CMOS chip for generating control signals for multiple qubits". *Nature Electronics*. **4** (4): 64–70. arXiv:1912.01299 (https://arxiv.org/abs/1912.01299). doi:10.1038/s41928-020-00528-y (https://doi.org/10.1038%2Fs41928-020-00528-y). S2CID 231715555 (https://api.semanticscholar.org/CorpusID:231715555).
15. "TdgGate" (https://qiskit.org/documentation/stubs/qiskit.circuit.library.TdgGate.html#qiskit.circuit.library.TdgGate). Qiskit online documentation.
16. "T dagger Gate" (https://www.quantum-inspire.com/kbase/t-dagger-gate/). cQASM online documentation.
17. Aharonov, Dorit (2003-01-09). "A Simple Proof that Toffoli and Hadamard are Quantum Universal". arXiv:quant-ph/0301040 (https://arxiv.org/abs/quant-ph/0301040).
18. Sawicki, Adam; Karnas, Katarzyna (2017-11-01). "Universality of Single-Qudit Gates" (https://doi.org/10.1007/s00023-017-0604-z). *Annales Henri Poincaré*. **18** (11): 3515–3552. arXiv:1609.05780 (https://arxiv.org/abs/1609.05780). Bibcode:2017AnHP...18.3515S (https://ui.adsabs.harvard.edu/abs/2017AnHP...18.3515S). doi:10.1007/s00023-017-0604-z (https://doi.org/10.1007%2Fs00023-017-0604-z). ISSN 1424-0661 (https://search.worldcat.org/issn/1424-0661). S2CID 253594045 (https://api.semanticscholar.org/CorpusID:253594045).
19. Sawicki, Adam; Mattioli, Lorenzo; Zimborás, Zoltán (2022-05-12). "Universality verification for a set of quantum gates" (https://link.aps.org/doi/10.1103/PhysRevA.105.052602). *Physical Review A*. **105** (5): 052602. arXiv:2111.03862 (https://arxiv.org/abs/2111.03862). Bibcode:2022PhRvA.105e2602S (https://ui.adsabs.harvard.edu/abs/2022PhRvA.105e2602S). doi:10.1103/PhysRevA.105.052602 (https://doi.org/10.1103%2FPhysRevA.105.052602). S2CID 248761038 (https://api.semanticscholar.org/CorpusID:248761038).
20. Williams, Colin P. (2011), Williams, Colin P. (ed.), "Quantum Gates" (https://doi.org/10.1007/978-1-84628-887-6_2), *Explorations in Quantum Computing*, Texts in Computer Science, London: Springer, pp. 51–122, doi:10.1007/978-1-84628-887-6_2 (https://doi.org/10.1007%2F978-1-84628-887-6_2), ISBN 978-1-84628-887-6, retrieved 2021-05-14
21. Deutsch, David (September 8, 1989), "Quantum computational networks", *Proc. R. Soc. Lond. A*, **425** (1989): 73–90, Bibcode:1989RSPSA.425...73D (https://ui.adsabs.harvard.edu/abs/1989RSPSA.425...73D), doi:10.1098/rspa.1989.0099 (https://doi.org/10.1098%2Frspa.1989.0099), S2CID 123073680 (https://api.semanticscholar.org/CorpusID:123073680)

22. Shi, Xiao-Feng (2018-05-22). "Deutsch, Toffoli, and cnot Gates via Rydberg Blockade of Neutral Atoms" (https://link.aps.org/doi/10.1103/PhysRevApplied.9.051001). *Physical Review Applied*. **9** (5): 051001. arXiv:1710.01859 (https://arxiv.org/abs/1710.01859). Bibcode:2018PhRvP...9e1001S (https://ui.adsabs.harvard.edu/abs/2018PhRvP...9e1001S). doi:10.1103/PhysRevApplied.9.051001 (https://doi.org/10.1103%2FPhysRevApplied.9.051001). ISSN 2331-7019 (https://search.worldcat.org/issn/2331-7019). S2CID 118909059 (https://api.semanticscholar.org/CorpusID:118909059).
23. "I operation" (https://docs.microsoft.com/en-us/qsharp/api/qsharp/microsoft.quantum.intrinsic.i). *docs.microsoft.com*. 28 July 2023.
24. "IGate" (https://qiskit.org/documentation/stubs/qiskit.circuit.library.IGate.html#qiskit.circuit.library.IGate). *qiskit.org*. Qiskit online documentation.
25. Loss, Daniel; DiVincenzo, David P. (1998-01-01). "Quantum computation with quantum dots" (https://doi.org/10.1103%2Fphysreva.57.120). *Physical Review A*. **57** (1): 120–126. arXiv:cond-mat/9701055 (https://arxiv.org/abs/cond-mat/9701055). Bibcode:1998PhRvA..57..120L (https://ui.adsabs.harvard.edu/abs/1998PhRvA..57..120L). doi:10.1103/physreva.57.120 (https://doi.org/10.1103%2Fphysreva.57.120). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). Example in eq. 2.
26. Raz, Ran (2002). "On the complexity of matrix product". *Proceedings of the thiry-fourth annual ACM Symposium on Theory of Computing*. pp. 144–151. doi:10.1145/509907.509932 (https://doi.org/10.1145%2F509907.509932). ISBN 1581134959. S2CID 9582328 (https://api.semanticscholar.org/CorpusID:9582328).
27. "UnitaryGate § UnitaryGate adjoint()" (https://docs.quantum.ibm.com/api/qiskit/qiskit.circuit.library.UnitaryGate#adjoint). *docs.quantum.ibm.com*.
28. Griffiths, D.J. (2008). *Introduction to Elementary Particles (2nd ed.)*. John Wiley & Sons. pp. 115–121, 126. ISBN 978-3-527-40601-2.
29. David Albert (1994). *Quantum mechanics and experience*. Harvard University Press. p. 35. ISBN 0-674-74113-7.
30. Sean M. Carroll (2019). *Spacetime and geometry: An introduction to general relativity*. Cambridge University Press. pp. 376–394. ISBN 978-1-108-48839-6.
31. David Wallace (2012). *The emergent multiverse: Quantum theory according to the Everett Interpretation*. Oxford University Press. ISBN 9780199546961.
32. Sean M. Carroll (2019). *Something deeply hidden: Quantum worlds and the emergence of spacetime*. Penguin Random House. ISBN 9781524743017.
33. Q# Online manual: Measurement (https://docs.microsoft.com/en-us/quantum/concepts/pauli-measurements)
34. Juan Yin; Yuan Cao; Yu-Huai Li; Sheng-Kai Liao; Liang Zhang; Ji-Gang Ren; Wen-Qi Cai; Wei-Yue Liu; Bo Li; Hui Dai; Guang-Bing Li; Qi-Ming Lu; Yun-Hong Gong; Yu Xu; Shuang-Lin Li; Feng-Zhi Li; Ya-Yun Yin; Zi-Qing Jiang; Ming Li; Jian-Jun Jia; Ge Ren; Dong He; Yi-Lin Zhou; Xiao-Xiang Zhang; Na Wang; Xiang Chang; Zhen-Cai Zhu; Nai-Le Liu; Yu-Ao Chen; Chao-Yang Lu; Rong Shu; Cheng-Zhi Peng; Jian-Yu Wang; Jian-Wei Pan (2017). "Satellite-based entanglement distribution over 1200 kilometers". *Quantum Optics*. **356** (6343): 1140–1144. arXiv:1707.01339 (https://arxiv.org/abs/1707.01339). doi:10.1126/science.aan3211 (https://doi.org/10.1126%2Fscience.aan3211). PMID 28619937 (https://pubmed.ncbi.nlm.nih.gov/28619937). S2CID 5206894 (https://api.semanticscholar.org/CorpusID:5206894).
35. Billings, Lee (23 April 2020). "China Shatters "Spooky Action at a Distance" Record, Preps for Quantum Internet" (https://www.scientificamerican.com/article/china-shatters-ldquo-spooky-action-at-a-distance-rdquo-record-preps-for-quantum-internet/). *Scientific American*.
36. Popkin, Gabriel (15 June 2017). "China's quantum satellite achieves 'spooky action' at record distance" (https://www.science.org/content/article/china-s-quantum-satellite-achieves-spooky-action-record-distance). *Science – AAAS*.
37. Aaronson, Scott (2009). "BQP and the Polynomial Hierarchy". arXiv:0910.4698 (https://arxiv.org/abs/0910.4698) [quant-ph (https://arxiv.org/archive/quant-ph)].
38. Dawson, Christopher M.; Nielsen, Michael (2006-01-01). "The Solovay-Kitaev algorithm" (https://dl.acm.org/doi/abs/10.5555/2011679.2011685). *Quantum Information and Computation*. **6** (1). Section 5.1, equation 23. arXiv:quant-ph/0505030 (https://arxiv.org/abs/quant-ph/0505030). doi:10.26421/QIC6.1-6 (https://doi.org/10.26421%2FQIC6.1-6).
39. Matteo, Olivia Di (2016). "Parallelizing quantum circuit synthesis" (https://dx.doi.org/10.1088/2058-9565/1/1/015003). *Quantum Science and Technology*. **1** (1): 015003. arXiv:1606.07413 (https://arxiv.org/abs/1606.07413). Bibcode:2016QS&T....1a5003D (https://ui.adsabs.harvard.edu/abs/2016QS&T....1a5003D). doi:10.1088/2058-9565/1/1/015003 (https://doi.org/10.1088%2F2058-9565%2F1%2F1%2F015003). S2CID 62819073 (https://api.semanticscholar.org/CorpusID:62819073).
40. Aaronson, Scott (2002). "Quantum Lower Bound for Recursive Fourier Sampling". *Quantum Information and Computation*. **3** (2): 165–174. arXiv:quant-ph/0209060 (https://arxiv.org/abs/quant-ph/0209060). Bibcode:2002quant.ph..9060A (https://ui.adsabs.harvard.edu/abs/2002quant.ph..9060A). doi:10.26421/QIC3.2-7 (https://doi.org/10.26421%2FQIC3.2-7).
41. Q# online manual: Quantum Memory Management (https://docs.microsoft.com/en-us/quantum/user-guide/language/statements/quantummemorymanagement?view=qsharp-preview)

42. Ryo, Asaka; Kazumitsu, Sakai; Ryoko, Yahagi (2020). "Quantum circuit for the fast Fourier transform" (https://link.springer.com/article/10.1007/s11128-020-02776-5). *Quantum Information Processing*. **19** (277): 277. arXiv:1911.03055 (https://arxiv.org/abs/1911.03055). Bibcode:2020QuIP...19..277A (https://ui.adsabs.harvard.edu/abs/2020QuIP...19..277A). doi:10.1007/s11128-020-02776-5 (https://doi.org/10.1007%2Fs11128-020-02776-5). S2CID 207847474 (https://api.semanticscholar.org/CorpusID:207847474).
43. Montaser, Rasha (2019). "New Design of Reversible Full Adder/Subtractor using R gate". *International Journal of Theoretical Physics*. **58** (1): 167–183. arXiv:1708.00306 (https://arxiv.org/abs/1708.00306). Bibcode:2019IJTP...58..167M (https://ui.adsabs.harvard.edu/abs/2019IJTP...58..167M). doi:10.1007/s10773-018-3921-1 (https://doi.org/10.1007%2Fs10773-018-3921-1). S2CID 24590164 (https://api.semanticscholar.org/CorpusID:24590164).
44. QCL 0.6.4 source code, the file "lib/examples.qcl" (http://tph.tuwien.ac.at/~oemer/tgz/qcl-0.6.4.tgz)

Sources

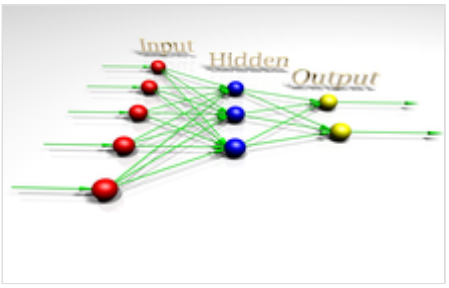
- Nielsen, Michael A.; Chuang, Isaac (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press. ISBN 0521632358. OCLC 43641333 (https://search.worldcat.org/oclc/43641333).
- Williams, Colin P. (2011). *Explorations in Quantum Computing*. Springer. ISBN 978-1-84628-887-6.
- Yanofsky, Noson S.; Mannucci, Mirco (2013). *Quantum computing for computer scientists*. Cambridge University Press. ISBN 978-0-521-87996-5.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_logic_gate&oldid=1240670066"

WIKIPEDIA
The Free Encyclopedia

Quantum neural network

Quantum neural networks are computational neural network models which are based on the principles of quantum mechanics. The first ideas on quantum neural computation were published independently in 1995 by Subhash Kak and Ron Chrisley,[1][2] engaging with the theory of quantum mind, which posits that quantum effects play a role in cognitive function. However, typical research in quantum neural networks involves combining classical artificial neural network models (which are widely used in machine learning for the important task of pattern recognition) with the advantages of quantum information in order to develop more efficient algorithms.[3][4][5] One important motivation for these investigations is the difficulty to train classical neural networks, especially in big data applications. The hope is that features of quantum computing such as quantum parallelism or the effects of interference and entanglement can be used as resources. Since the technological implementation of a quantum computer is still in a premature stage, such quantum neural network models are mostly theoretical proposals that await their full implementation in physical experiments.



Simple model of a feed forward neural network. For a deep learning network, increase the number of hidden layers.

Most Quantum neural networks are developed as feed-forward networks. Similar to their classical counterparts, this structure intakes input from one layer of qubits, and passes that input onto another layer of qubits. This layer of qubits evaluates this information and passes on the output to the next layer. Eventually the path leads to the final layer of qubits.[6][7] The layers do not have to be of the same width, meaning they don't have to have the same number of qubits as the layer before or after it. This structure is trained on which path to take similar to classical artificial neural networks. This is discussed in a lower section. Quantum neural networks refer to three different categories: Quantum computer with classical data, classical computer with quantum data, and quantum computer with quantum data.[6]

Examples

Quantum neural network research is still in its infancy, and a conglomeration of proposals and ideas of varying scope and mathematical rigor have been put forward. Most of them are based on the idea of replacing classical binary or McCulloch-Pitts neurons with a qubit (which can be called a “quron”), resulting in neural units that can be in a superposition of the state ‘firing’ and ‘resting’.

Quantum perceptrons

A lot of proposals attempt to find a quantum equivalent for the perceptron unit from which neural nets are constructed. A problem is that nonlinear activation functions do not immediately correspond to the mathematical structure of quantum theory, since a quantum evolution is described by linear operations and leads to probabilistic observation. Ideas to imitate the perceptron activation function with a quantum mechanical formalism reach from special measurements [8][9] to postulating non-linear quantum operators

(a mathematical framework that is disputed).[10][11] A direct implementation of the activation function using the circuit-based model of quantum computation has recently been proposed by Schuld, Sinayskiy and Petruccione based on the quantum phase estimation algorithm.[12]

Quantum networks

At a larger scale, researchers have attempted to generalize neural networks to the quantum setting. One way of constructing a quantum neuron is to first generalise classical neurons and then generalising them further to make unitary gates. Interactions between neurons can be controlled quantumly, with unitary gates, or classically, via measurement of the network states. This high-level theoretical technique can be applied broadly, by taking different types of networks and different implementations of quantum neurons, such as photonically implemented neurons[7][13] and quantum reservoir processor (quantum version of reservoir computing).[14] Most learning algorithms follow the classical model of training an artificial neural network to learn the input-output function of a given training set and use classical feedback loops to update parameters of the quantum system until they converge to an optimal configuration. Learning as a parameter optimisation problem has also been approached by adiabatic models of quantum computing.[15]

Quantum neural networks can be applied to algorithmic design: given qubits with tunable mutual interactions, one can attempt to learn interactions following the classical backpropagation rule from a training set of desired input-output relations, taken to be the desired output algorithm's behavior.[16][17] The quantum network thus ‘learns’ an algorithm.

Quantum associative memory

The first quantum associative memory algorithm was introduced by Dan Ventura and Tony Martinez in 1999.[18] The authors do not attempt to translate the structure of artificial neural network models into quantum theory, but propose an algorithm for a circuit-based quantum computer that simulates associative memory. The memory states (in Hopfield neural networks saved in the weights of the neural connections) are written into a superposition, and a Grover-like quantum search algorithm retrieves the memory state closest to a given input. As such, this is not a fully content-addressable memory, since only incomplete patterns can be retrieved.

The first truly content-addressable quantum memory, which can retrieve patterns also from corrupted inputs, was proposed by Carlo A. Trugenberger.[19][20][21] Both memories can store an exponential (in terms of n qubits) number of patterns but can be used only once due to the no-cloning theorem and their destruction upon measurement.

Trugenberger,[20] however, has shown that his proabilistic model of quantum associative memory can be efficiently implemented and re-used multiples times for any polynomial number of stored patterns, a large advantage with respect to classical associative memories.

Classical neural networks inspired by quantum theory

A substantial amount of interest has been given to a “quantum-inspired” model that uses ideas from quantum theory to implement a neural network based on fuzzy logic.[22]

Training

Quantum Neural Networks can be theoretically trained similarly to training classical/artificial neural networks. A key difference lies in communication between the layers of a neural networks. For classical neural networks, at the end of a given operation, the current perceptron copies its output to the next layer of perceptron(s) in the network. However, in a quantum neural network, where each perceptron is a qubit, this would violate the no-cloning theorem.[6][23] A proposed generalized solution to this is to replace the classical fan-out method with an arbitrary unitary that spreads out, but does not copy, the output of one qubit to the next layer of qubits. Using this fan-out Unitary (U_f) with a dummy state qubit in a known state (Ex. $|0\rangle$ in the computational basis), also known as an Ancilla bit, the information from the qubit can be transferred to the next layer of qubits.[7] This process adheres to the quantum operation requirement of reversibility.[7][24]

Using this quantum feed-forward network, deep neural networks can be executed and trained efficiently. A deep neural network is essentially a network with many hidden-layers, as seen in the sample model neural network above. Since the Quantum neural network being discussed uses fan-out Unitary operators, and each operator only acts on its respective input, only two layers are used at any given time.[6] In other words, no Unitary operator is acting on the entire network at any given time, meaning the number of qubits required for a given step depends on the number of inputs in a given layer. Since Quantum Computers are notorious for their ability to run multiple iterations in a short period of time, the efficiency of a quantum neural network is solely dependent on the number of qubits in any given layer, and not on the depth of the network.[24]

Cost functions

To determine the effectiveness of a neural network, a cost function is used, which essentially measures the proximity of the network's output to the expected or desired output. In a Classical Neural Network, the weights (w) and biases (b) at each step determine the outcome of the cost function $C(w,b)$.[6] When training a Classical Neural network, the weights and biases are adjusted after each iteration, and given equation 1 below, where $y(x)$ is the desired output and $a^{\text{out}}(x)$ is the actual output, the cost function is optimized when $C(w,b)$= 0. For a quantum neural network, the cost function is determined by measuring the fidelity of the outcome state (ρ^{out}) with the desired outcome state (ϕ^{out}), seen in Equation 2 below. In this case, the Unitary operators are adjusted after each iteration, and the cost function is optimized when C = 1.[6]

Equation 1 $$C(w,b) = \frac{1}{N}\sum_{x}\frac{||y(x) - a^{\text{out}}(x)||}{2}$$

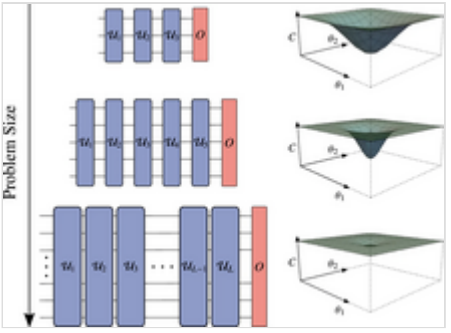
Equation 2 $C = \frac{1}{N}\sum_{x}^{N}\langle \phi^{\text{out}}|\rho^{\text{out}}|\phi^{\text{out}}\rangle$

Barren plateaus

Gradient descent is widely used and successful in classical algorithms. However, although the simplified structure is very similar to neural networks such as CNNs, QNNs perform much worse.

Since the quantum space exponentially expands as the q-bit grows, the observations will concentrate around the mean value at an exponential rate, where also have exponentially small gradients.[26]

This situation is known as Barren Plateaus, because most of the initial parameters are trapped on a "plateau" of almost zero gradient, which approximates random wandering[26] rather than gradient descent. This makes the model untrainable.



Barren plateaus of VQA[25] Figure shows the Barren Plateau problem becomes increasingly serious as the VQA expands.

In fact, not only QNN, but almost all deeper VQA algorithms have this problem. In the present NISQ era, this is one of the problems that have to be solved if more applications are to be made of the various VQA algorithms, including QNN.

See also

- Differentiable programming
- Optical neural network
- Holographic associative memory
- Quantum cognition
- Quantum machine learning

References

1. Kak, S. (1995). "On quantum neural computing". *Advances in Imaging and Electron Physics*. **94**: 259–313. doi:10.1016/S1076-5670(08)70147-2 (https://doi.org/10.1016%2FS1076-5670%2808%2970147-2). ISBN 9780120147366.
2. Chrisley, R. (1995). "Quantum Learning". In Pylkkänen, P.; Pylkkö, P. (eds.). *New directions in cognitive science: Proceedings of the international symposium, Saariselka, 4–9 August 1995, Lapland, Finland*. Helsinki: Finnish Association of Artificial Intelligence. pp. 77–89. ISBN 951-22-2645-6.

3. da Silva, Adenilton J.; Ludermir, Teresa B.; de Oliveira, Wilson R. (2016). "Quantum perceptron over a field and neural network architecture selection in a quantum computer". *Neural Networks*. **76**: 55–64. arXiv:1602.00709 (https://arxiv.org/abs/1602.00709). Bibcode:2016arXiv160200709D (https://ui.adsabs.harvard.edu/abs/2016arXiv160200709D). doi:10.1016/j.neunet.2016.01.002 (https://doi.org/10.1016%2Fj.neunet.2016.01.002). PMID 26878722 (https://pubmed.ncbi.nlm.nih.gov/26878722). S2CID 15381014 (https://api.semanticscholar.org/CorpusID:15381014).
4. Panella, Massimo; Martinelli, Giuseppe (2011). "Neural networks with quantum architecture and quantum learning". *International Journal of Circuit Theory and Applications*. **39**: 61–77. doi:10.1002/cta.619 (https://doi.org/10.1002%2Fcta.619). S2CID 3791858 (https://api.semanticscholar.org/CorpusID:3791858).
5. Schuld, M.; Sinayskiy, I.; Petruccione, F. (2014). "The quest for a Quantum Neural Network". *Quantum Information Processing*. **13** (11): 2567–2586. arXiv:1408.7005 (https://arxiv.org/abs/1408.7005). Bibcode:2014QuIP...13.2567S (https://ui.adsabs.harvard.edu/abs/2014QuIP...13.2567S). doi:10.1007/s11128-014-0809-8 (https://doi.org/10.1007%2Fs11128-014-0809-8). S2CID 37238534 (https://api.semanticscholar.org/CorpusID:37238534).
6. Beer, Kerstin; Bondarenko, Dmytro; Farrelly, Terry; Osborne, Tobias J.; Salzmann, Robert; Scheiermann, Daniel; Wolf, Ramona (2020-02-10). "Training deep quantum neural networks" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7010779). *Nature Communications*. **11** (1): 808. arXiv:1902.10445 (https://arxiv.org/abs/1902.10445). Bibcode:2020NatCo..11..808B (https://ui.adsabs.harvard.edu/abs/2020NatCo..11..808B). doi:10.1038/s41467-020-14454-2 (https://doi.org/10.1038%2Fs41467-020-14454-2). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 7010779 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7010779). PMID 32041956 (https://pubmed.ncbi.nlm.nih.gov/32041956).
7. Wan, Kwok-Ho; Dahlsten, Oscar; Kristjansson, Hler; Gardner, Robert; Kim, Myungshik (2017). "Quantum generalisation of feedforward neural networks". *npj Quantum Information*. **3**: 36. arXiv:1612.01045 (https://arxiv.org/abs/1612.01045). Bibcode:2017npjQI...3...36W (https://ui.adsabs.harvard.edu/abs/2017npjQI...3...36W). doi:10.1038/s41534-017-0032-4 (https://doi.org/10.1038%2Fs41534-017-0032-4). S2CID 51685660 (https://api.semanticscholar.org/CorpusID:51685660).
8. Perus, M. (2000). "Neural Networks as a basis for quantum associative memory". *Neural Network World*. **10** (6): 1001. CiteSeerX 10.1.1.106.4583 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.106.4583).
9. Zak, M.; Williams, C. P. (1998). "Quantum Neural Nets". *International Journal of Theoretical Physics*. **37** (2): 651–684. doi:10.1023/A:1026656110699 (https://doi.org/10.1023%2FA%3A1026656110699). S2CID 55783801 (https://api.semanticscholar.org/CorpusID:55783801).
10. Gupta, Sanjay; Zia, R.K.P. (2001). "Quantum Neural Networks". *Journal of Computer and System Sciences*. **63** (3): 355–383. arXiv:quant-ph/0201144 (https://arxiv.org/abs/quant-ph/0201144). doi:10.1006/jcss.2001.1769 (https://doi.org/10.1006%2Fjcss.2001.1769). S2CID 206569020 (https://api.semanticscholar.org/CorpusID:206569020).
11. Faber, J.; Giraldi, G. A. (2002). "Quantum Models for Artificial Neural Network" (http://virtual01.lncc.br/~giraldi/TechReport/QNN-Review.pdf.gz).
12. Schuld, M.; Sinayskiy, I.; Petruccione, F. (2014). "Simulating a perceptron on a quantum computer". *Physics Letters A*. **379** (7): 660–663. arXiv:1412.3635 (https://arxiv.org/abs/1412.3635). doi:10.1016/j.physleta.2014.11.061 (https://doi.org/10.1016%2Fj.physleta.2014.11.061). S2CID 14288234 (https://api.semanticscholar.org/CorpusID:14288234).
13. Narayanan, A.; Menneer, T. (2000). "Quantum artificial neural network architectures and components". *Information Sciences*. **128** (3–4): 231–255. doi:10.1016/S0020-0255(00)00055-4 (https://doi.org/10.1016%2FS0020-0255%2800%2900055-4). S2CID 10901562 (https://api.semanticscholar.org/CorpusID:10901562).

14. Ghosh, S.; Opala, A.; Matuszewski, M.; Paterek, P.; Liew, T. C. H. (2019). "Quantum reservoir processing". *npj Quantum Information*. **5**: 35. arXiv:1811.10335 (https://arxiv.org/abs/1811.10335). Bibcode:2019npjQI...5...35G (https://ui.adsabs.harvard.edu/abs/2019npjQI...5...35G). doi:10.1038/s41534-019-0149-8 (https://doi.org/10.1038%2Fs41534-019-0149-8). S2CID 119197635 (https://api.semanticscholar.org/CorpusID:119197635).
15. Neven, H.; et al. (2008). "Training a Binary Classifier with the Quantum Adiabatic Algorithm". arXiv:0811.0416 (https://arxiv.org/abs/0811.0416) [quant-ph (https://arxiv.org/archive/quant-ph)].
16. Bang, J.; et al. (2014). "A strategy for quantum algorithm design assisted by machine learning". *New Journal of Physics*. **16** (7): 073017. arXiv:1301.1132 (https://arxiv.org/abs/1301.1132). Bibcode:2014NJPh...16g3017B (https://ui.adsabs.harvard.edu/abs/2014NJPh...16g3017B). doi:10.1088/1367-2630/16/7/073017 (https://doi.org/10.1088%2F1367-2630%2F16%2F7%2F073017). S2CID 55377982 (https://api.semanticscholar.org/CorpusID:55377982).
17. Behrman, E. C.; Steck, J. E.; Kumar, P.; Walsh, K. A. (2008). "Quantum Algorithm design using dynamic learning". *Quantum Information and Computation*. **8** (1–2): 12–29. arXiv:0808.1558 (https://arxiv.org/abs/0808.1558). doi:10.26421/QIC8.1-2-2 (https://doi.org/10.26421%2FQIC8.1-2-2). S2CID 18587557 (https://api.semanticscholar.org/CorpusID:18587557).
18. Ventura, D.; Martinez, T. (1999). "A Quantum Associative Memory Based on Grover's Algorithm" (https://web.archive.org/web/20170911115617/https://pdfs.semanticscholar.org/d46f/e04b57b75a7f9c57f25d03d1c56b480ab755.pdf) (PDF). *Artificial Neural Nets and Genetic Algorithms*. pp. 22–27. doi:10.1007/978-3-7091-6384-9_5 (https://doi.org/10.1007%2F978-3-7091-6384-9_5). ISBN 978-3-211-83364-3. S2CID 3258510 (https://api.semanticscholar.org/CorpusID:3258510). Archived from the original (https://pdfs.semanticscholar.org/d46f/e04b57b75a7f9c57f25d03d1c56b480ab755.pdf) (PDF) on 2017-09-11.
19. Trugenberger, C. A. (2001-07-18). "Probabilistic Quantum Memories" (https://dx.doi.org/10.1103/physrevlett.87.067901). *Physical Review Letters*. **87** (6): 067901. arXiv:quant-ph/0012100 (https://arxiv.org/abs/quant-ph/0012100). Bibcode:2001PhRvL..87f7901T (https://ui.adsabs.harvard.edu/abs/2001PhRvL..87f7901T). doi:10.1103/physrevlett.87.067901 (https://doi.org/10.1103%2Fphysrevlett.87.067901). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 11497863 (https://pubmed.ncbi.nlm.nih.gov/11497863). S2CID 23325931 (https://api.semanticscholar.org/CorpusID:23325931).
20. Trugenberger, Carlo A. (2002). "Quantum Pattern Recognition". *Quantum Information Processing*. **1** (6): 471–493. doi:10.1023/A:1024022632303 (https://doi.org/10.1023%2FA%3A1024022632303). S2CID 1928001 (https://api.semanticscholar.org/CorpusID:1928001).
21. Trugenberger, C. A. (2002-12-19). "Phase Transitions in Quantum Pattern Recognition" (https://dx.doi.org/10.1103/physrevlett.89.277903). *Physical Review Letters*. **89** (27): 277903. arXiv:quant-ph/0204115 (https://arxiv.org/abs/quant-ph/0204115). Bibcode:2002PhRvL..89A7903T (https://ui.adsabs.harvard.edu/abs/2002PhRvL..89A7903T). doi:10.1103/physrevlett.89.277903 (https://doi.org/10.1103%2Fphysrevlett.89.277903). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 12513243 (https://pubmed.ncbi.nlm.nih.gov/12513243). S2CID 33065081 (https://api.semanticscholar.org/CorpusID:33065081).
22. Purushothaman, G.; Karayiannis, N. (1997). "Quantum Neural Networks (QNN's): Inherently Fuzzy Feedforward Neural Networks" (https://web.archive.org/web/20170911115935/https://pdfs.semanticscholar.org/fe11/93d386f42358e7cf9b1f71bf33e7ddd945b5.pdf) (PDF). *IEEE Transactions on Neural Networks*. **8** (3): 679–93. doi:10.1109/72.572106 (https://doi.org/10.1109%2F72.572106). PMID 18255670 (https://pubmed.ncbi.nlm.nih.gov/18255670). S2CID 1634670 (https://api.semanticscholar.org/CorpusID:1634670). Archived from the original (https://pdfs.semanticscholar.org/fe11/93d386f42358e7cf9b1f71bf33e7ddd945b5.pdf) (PDF) on 2017-09-11.

23. Nielsen, Michael A; Chuang, Isaac L (2010). *Quantum computation and quantum information* (https://www.worldcat.org/oclc/665137861). Cambridge; New York: Cambridge University Press. ISBN 978-1-107-00217-3. OCLC 665137861 (https://search.worldcat.org/oclc/665137861).
24. Feynman, Richard P. (1986-06-01). "Quantum mechanical computers" (https://doi.org/10.1007/BF01886518). *Foundations of Physics*. **16** (6): 507–531. Bibcode:1986FoPh...16..507F (https://ui.adsabs.harvard.edu/abs/1986FoPh...16..507F). doi:10.1007/BF01886518 (https://doi.org/10.1007%2FBF01886518). ISSN 1572-9516 (https://search.worldcat.org/issn/1572-9516). S2CID 122076550 (https://api.semanticscholar.org/CorpusID:122076550).
25. Wang, Samson; Fontana, Enrico; Cerezo, M.; Sharma, Kunal; Sone, Akira; Cincio, Lukasz; Coles, Patrick J. (2021-11-29). "Noise-induced barren plateaus in variational quantum algorithms" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8630047). *Nature Communications*. **12** (1): 6961. arXiv:2007.14384 (https://arxiv.org/abs/2007.14384). Bibcode:2021NatCo..12.6961W (https://ui.adsabs.harvard.edu/abs/2021NatCo..12.6961W). doi:10.1038/s41467-021-27045-6 (https://doi.org/10.1038%2Fs41467-021-27045-6). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 8630047 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8630047). PMID 34845216 (https://pubmed.ncbi.nlm.nih.gov/34845216).
26. McClean, Jarrod R.; Boixo, Sergio; Smelyanskiy, Vadim N.; Babbush, Ryan; Neven, Hartmut (2018-11-16). "Barren plateaus in quantum neural network training landscapes" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6240101). *Nature Communications*. **9** (1): 4812. arXiv:1803.11173 (https://arxiv.org/abs/1803.11173). Bibcode:2018NatCo...9.4812M (https://ui.adsabs.harvard.edu/abs/2018NatCo...9.4812M). doi:10.1038/s41467-018-07090-4 (https://doi.org/10.1038%2Fs41467-018-07090-4). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 6240101 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6240101). PMID 30446662 (https://pubmed.ncbi.nlm.nih.gov/30446662).

External links

- Recent review of quantum neural networks by M. Schuld, I. Sinayskiy and F. Petruccione (https://arxiv.org/abs/1408.7005)
- Review of quantum neural networks by Wei (http://www.cic.unb.br/~weigang/qc/aci.html)
- Article by P. Gralewicz on the plausibility of quantum computing in biological neural networks (https://arxiv.org/abs/quant-ph/0401127)
- Training a neural net to recognize images (https://web.archive.org/web/20131113014007/http://www.dwavesys.com/en/dev-tutorial-neural.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_neural_network&oldid=1242603622"

WIKIPEDIA
The Free Encyclopedia

Quantum Turing machine

A **quantum Turing machine** (**QTM**) or **universal quantum computer** is an abstract machine used to model the effects of a quantum computer. It provides a simple model that captures all of the power of quantum computation—that is, any quantum algorithm can be expressed formally as a particular quantum Turing machine. However, the computationally equivalent quantum circuit is a more common model.[1][2]:2

Quantum Turing machines can be related to classical and probabilistic Turing machines in a framework based on transition matrices. That is, a matrix can be specified whose product with the matrix representing a classical or probabilistic machine provides the quantum probability matrix representing the quantum machine. This was shown by Lance Fortnow.[3]

Informal sketch

Unsolved problem in physics:

? *Is a universal quantum computer sufficient to efficiently simulate an arbitrary physical system?*

(more unsolved problems in physics)

A way of understanding the quantum Turing machine (QTM) is that it generalizes the classical Turing machine (TM) in the same way that the quantum finite automaton (QFA) generalizes the deterministic finite automaton (DFA). In essence, the internal states of a classical TM are replaced by pure or mixed states in a Hilbert space; the transition function is replaced by a collection of unitary matrices that map the Hilbert space to itself.[4]

That is, a classical Turing machine is described by a 7-tuple $M = \langle Q, \Gamma, b, \Sigma, \delta, q_0, F \rangle$.

For a three-tape quantum Turing machine (one tape holding the input, a second tape holding intermediate calculation results, and a third tape holding output):

- The set of states Q is replaced by a Hilbert space.
- The tape alphabet symbols Γ are likewise replaced by a Hilbert space (usually a different Hilbert space than the set of states).
- The blank symbol $b \in \Gamma$ is an element of the Hilbert space.
- The input and output symbols Σ are usually taken as a discrete set, as in the classical system; thus, neither the input nor output to a quantum machine need be a quantum system itself.
- The transition function $\delta : \Sigma \times Q \otimes \Gamma \to \Sigma \times Q \otimes \Gamma \times \{L, R\}$ is a generalization of a transition monoid and is understood to be a collection of unitary matrices that are automorphisms of the Hilbert space Q.
- The initial state $q_0 \in Q$ may be either a mixed state or a pure state.
- The set F of *final* or *accepting states* is a subspace of the Hilbert space Q.

The above is merely a sketch of a quantum Turing machine, rather than its formal definition, as it leaves vague several important details: for example, how often a measurement is performed; see for example, the difference between a measure-once and a measure-many QFA. This question of measurement affects the way in which writes to the output tape are defined.

History

In 1980 and 1982, physicist Paul Benioff published articles[5][6] that first described a quantum mechanical model of Turing machines. A 1985 article written by Oxford University physicist David Deutsch further developed the idea of quantum computers by suggesting that quantum gates could function in a similar fashion to traditional digital computing binary logic gates.[4]

Iriyama, Ohya, and Volovich have developed a model of a *linear quantum Turing machine* (LQTM). This is a generalization of a classical QTM that has mixed states and that allows irreversible transition functions. These allow the representation of quantum measurements without classical outcomes.[7]

A *quantum Turing machine with postselection* was defined by Scott Aaronson, who showed that the class of polynomial time on such a machine (PostBQP) is equal to the classical complexity class PP.[8]

See also

- Quantum simulator § Solving physics problems

References

1. Andrew Yao (1993). *Quantum circuit complexity*. 34th Annual Symposium on Foundations of Computer Science. pp. 352–361.
2. Abel Molina; John Watrous (2018). "Revisiting the simulation of quantum Turing machines by quantum circuits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598068). *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. **475** (2226). arXiv:1808.01701 (https://arxiv.org/abs/1808.01701). doi:10.1098/rspa.2018.0767 (https://doi.org/10.1098%2Frspa.2018.0767). PMC 6598068 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598068). PMID 31293355 (https://pubmed.ncbi.nlm.nih.gov/31293355).
3. Fortnow, Lance (2003). "One Complexity Theorist's View of Quantum Computing". *Theoretical Computer Science*. **292** (3): 597–610. arXiv:quant-ph/0003035 (https://arxiv.org/abs/quant-ph/0003035). doi:10.1016/S0304-3975(01)00377-2 (https://doi.org/10.1016%2FS0304-3975%2801%2900377-2). S2CID 18657540 (https://api.semanticscholar.org/CorpusID:18657540).
4. Deutsch, David (July 1985). "Quantum theory, the Church-Turing principle and the universal quantum computer" (https://web.archive.org/web/20081123183419/http://www.ceid.upatras.gr/tech_news/papers/quantum_theory.pdf) (PDF). *Proceedings of the Royal Society A*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D (https://ui.adsabs.harvard.edu/abs/1985RSPSA.400...97D). CiteSeerX 10.1.1.41.2382 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.2382). doi:10.1098/rspa.1985.0070 (https://doi.org/10.1098%2Frspa.1985.0070). S2CID 1438116 (https://api.semanticscholar.org/CorpusID:1438116). Archived from the original (http://www.ceid.upatras.gr/tech_news/papers/quantum_theory.pdf) (PDF) on 2008-11-23.

5. Benioff, Paul (1980). "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines". *Journal of Statistical Physics*. **22** (5): 563–591. Bibcode:1980JSP....22..563B (https://ui.adsabs.harvard.edu/abs/1980JSP....22..563B). doi:10.1007/bf01011339 (https://doi.org/10.1007%2Fbf01011339). S2CID 122949592 (https://api.semanticscholar.org/CorpusID:122949592).
6. Benioff, P. (1982). "Quantum mechanical hamiltonian models of turing machines". *Journal of Statistical Physics*. **29** (3): 515–546. Bibcode:1982JSP....29..515B (https://ui.adsabs.harvard.edu/abs/1982JSP....29..515B). doi:10.1007/BF01342185 (https://doi.org/10.1007%2FBF01342185). S2CID 14956017 (https://api.semanticscholar.org/CorpusID:14956017).
7. Simon Perdrix; Philippe Jorrand (2007-04-04). "Classically Controlled Quantum Computation". *Math. Struct. In Comp. Science*. **16** (4): 601–620. arXiv:quant-ph/0407008 (https://arxiv.org/abs/quant-ph/0407008). doi:10.1017/S096012950600538X (https://doi.org/10.1017%2FS096012950600538X). S2CID 16142327 (https://api.semanticscholar.org/CorpusID:16142327). Also: Simon Perdrix and Philippe Jorrand (2006). "Classically-Controlled Quantum Computation" (http://dcm-workshop.org.uk./2005/dcm-draft-proceedings.pdf) (PDF). *Math. Struct. In Comp. Science*. **16** (4): 601–620. arXiv:quant-ph/0407008 (https://arxiv.org/abs/quant-ph/0407008). CiteSeerX 10.1.1.252.1823 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.252.1823). doi:10.1017/S096012950600538X (https://doi.org/10.1017%2FS096012950600538X). S2CID 16142327 (https://api.semanticscholar.org/CorpusID:16142327).
8. Aaronson, Scott (2005). "Quantum computing, postselection, and probabilistic polynomial-time". *Proceedings of the Royal Society A*. **461** (2063): 3473–3482. arXiv:quant-ph/0412187 (https://arxiv.org/abs/quant-ph/0412187). Bibcode:2005RSPSA.461.3473A (https://ui.adsabs.harvard.edu/abs/2005RSPSA.461.3473A). doi:10.1098/rspa.2005.1546 (https://doi.org/10.1098%2Frspa.2005.1546). S2CID 1770389 (https://api.semanticscholar.org/CorpusID:1770389). Preprint available at [1] (https://arxiv.org/abs/quant-ph/0412187).

Further reading

- Molina, Abel; Watrous, John (2018). "Revisiting the simulation of quantum Turing machines by quantum circuits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598068). *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*. **475** (2226). arXiv:1808.01701 (https://arxiv.org/abs/1808.01701). doi:10.1098/rspa.2018.0767 (https://doi.org/10.1098%2Frspa.2018.0767). PMC 6598068 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6598068). PMID 31293355 (https://pubmed.ncbi.nlm.nih.gov/31293355).
- Iriyama, Satoshi; Ohya, Masanori; Volovich, Igor (2004). "Generalized Quantum Turing Machine and its Application to the SAT Chaos Algorithm". arXiv:quant-ph/0405191 (https://arxiv.org/abs/quant-ph/0405191).
- Deutsch, D. (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D (https://ui.adsabs.harvard.edu/abs/1985RSPSA.400...97D). CiteSeerX 10.1.1.41.2382 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.41.2382). doi:10.1098/rspa.1985.0070 (https://doi.org/10.1098%2Frspa.1985.0070). JSTOR 2397601 (https://www.jstor.org/stable/2397601). S2CID 1438116 (https://api.semanticscholar.org/CorpusID:1438116).

External links

- The quantum computer – history (http://ffden-2.phys.uaf.edu/211.web.stuff/Almeida/history.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_Turing_machine&oldid=1094087087"

WIKIPEDIA
The Free Encyclopedia

Topological quantum computer

A **topological quantum computer** is a theoretical quantum computer proposed by Russian-American physicist Alexei Kitaev in 1997.[1] It employs quasiparticles in two-dimensional systems, called anyons, whose world lines pass around one another to form braids in a three-dimensional spacetime (i.e., one temporal plus two spatial dimensions). These braids form the logic gates that make up the computer. The advantage of a quantum computer based on quantum braids over using trapped quantum particles is that the former is much more stable. Small, cumulative perturbations can cause quantum states to decohere and introduce errors in the computation, but such small perturbations do not change the braids' topological properties. This is like the effort required to cut a string and reattach the ends to form a different braid, as opposed to a ball (representing an ordinary quantum particle in four-dimensional spacetime) bumping into a wall.

While the elements of a topological quantum computer originate in a purely mathematical realm, experiments in fractional quantum Hall systems indicate these elements may be created in the real world using semiconductors made of gallium arsenide at a temperature of near absolute zero and subjected to strong magnetic fields.

Microsoft is the only major technology company with a history of research and development in topological quantum computing.[2][3]

In 2023, Microsoft researchers published a paper in Physical Review that described a new device that can represent a logical qubit with hardware stability, measuring a phase of matter consistent with the observation of topological superconductivity and Majorana zero modes.[4] The scientists reported that "such devices have demonstrated low enough disorder to pass the topological gap protocol, proving the technology is viable."[5]

Introduction

Anyons are quasiparticles in a two-dimensional space. Anyons are neither fermions nor bosons, but like fermions, they cannot occupy the same state. Thus, the world lines of two anyons cannot intersect or merge, which allows their paths to form stable braids in space-time. Anyons can form from excitations in a cold, two-dimensional electron gas in a very strong magnetic field, and carry fractional units of magnetic flux. This phenomenon is called the fractional quantum Hall effect. In typical laboratory systems, the electron gas occupies a thin semiconducting layer sandwiched between layers of aluminium gallium arsenide.

When anyons are braided, the transformation of the quantum state of the system depends only on the topological class of the anyons' trajectories (which are classified according to the braid group). Therefore, the quantum information which is stored in the state of the system is impervious to small errors in the trajectories.[6] In 2005, Sankar Das Sarma, Michael Freedman, and Chetan Nayak proposed a quantum Hall device that would realize a topological qubit. In 2005 Vladimir J. Goldman, Fernando E. Camino, and Wei Zhou[7] claimed to have created and observed the first experimental evidence for using a

fractional quantum Hall effect to create actual anyons, although others have suggested their results could be the product of phenomena not involving anyons. Non-abelian anyons, a species required for topological quantum computers, have yet to be experimentally confirmed. Possible experimental evidence has been found,[8] but the conclusions remain contested.[9] In 2018, scientists again claimed to have isolated the required Majorana particles, but the finding was retracted in 2021. *Quanta Magazine* stated in 2021 that "no one has convincingly shown the existence of even a single (Majorana zero-mode) quasiparticle",[10] although in 2023 a new article[11] by the magazine has covered some preprints by Google[12] and Quantinuum[13] claiming the realization of non-abelian anyons on quantum processors, the first used a toric code with twist defects as a topological degenerancy (or topological defect) while the second used a different but related protocol both of which can be understood as Majorana bound states in quantum error correction.

Topological vs. standard quantum computer

Topological quantum computers are equivalent in computational power to other standard models of quantum computation, in particular to the quantum circuit model and to the quantum Turing machine model.[14] That is, any of these models can efficiently simulate any of the others. Nonetheless, certain algorithms may be a more natural fit to the topological quantum computer model. For example, algorithms for evaluating the Jones polynomial were first developed in the topological model, and only later converted and extended in the standard quantum circuit model.

Computations

To live up to its name, a topological quantum computer must provide the unique computation properties promised by a conventional quantum computer design, which uses trapped quantum particles. In 2000, Michael H. Freedman, Alexei Kitaev, Michael J. Larsen, and Zhenghan Wang proved that a topological quantum computer can, in principle, perform any computation that a conventional quantum computer can do, and vice versa.[14][15][16]

They found that a conventional quantum computer device, given an error-free operation of its logic circuits, will give a solution with an absolute level of accuracy, whereas a topological quantum computing device with flawless operation will give the solution with only a finite level of accuracy. However, any level of precision for the answer can be obtained by adding more braid twists (logic circuits) to the topological quantum computer, in a simple linear relationship. In other words, a reasonable increase in elements (braid twists) can achieve a high degree of accuracy in the answer. Actual computation [gates] are done by the edge states of a fractional quantum Hall effect. This makes models of one-dimensional anyons important. In one space dimension, anyons are defined algebraically.

Error correction and control

Even though quantum braids are inherently more stable than trapped quantum particles, there is still a need to control for error inducing thermal fluctuations, which produce random stray pairs of anyons which interfere with adjoining braids. Controlling these errors is simply a matter of separating the anyons to a distance where the rate of interfering strays drops to near zero. Simulating the dynamics of a

topological quantum computer may be a promising method of implementing fault-tolerant quantum computation even with a standard quantum information processing scheme. Raussendorf, Harrington, and Goyal have studied one model, with promising simulation results.[17]

Example: Computing with Fibonacci anyons

One of the prominent examples in topological quantum computing is with a system of Fibonacci anyons. A Fibonacci anyon has been described as "an emergent particle with the property that as you add more particles to the system, the number of quantum states grows like the Fibonacci sequence, 1, 2, 3, 5, 8, etc.."[18] In the context of conformal field theory, fibonacci anyons are described by the Yang–Lee model, the SU(2) special case of the Chern–Simons theory and Wess–Zumino–Witten models.[19] These anyons can be used to create generic gates for topological quantum computing. There are three main steps for creating a model:

- Choose our basis and restrict our Hilbert space
- Braid the anyons together
- Fuse the anyons at the end, and detect how they fuse in order to read the output of the system.

State preparation

Fibonacci anyons are defined by three qualities:

1. They have a topological charge of τ. In this discussion, we consider another charge called 1 which is the ‘vacuum’ charge if anyons are annihilated with each-other.
2. Each of these anyons are their own antiparticle. $\tau = \tau^*$ and $1 = 1^*$.
3. If brought close to each-other, they will ‘fuse’ together in a nontrivial fashion. Specifically, the ‘fusion’ rules are:
    1. $1 \otimes 1 = 1$
    2. $1 \otimes \tau = \tau \otimes 1 = \tau$
    3. $\tau \otimes \tau = 1 \oplus \tau$
4. Many of the properties of this system can be explained similarly to that of two spin 1/2 particles. Particularly, we use the same tensor product $\otimes$ and direct sum $\oplus$ operators.

The last ‘fusion’ rule can be extended this to a system of three anyons:

$$\tau \otimes \tau \otimes \tau = \tau \otimes (1 \oplus \tau) = \tau \otimes 1 \oplus \tau \otimes \tau = \tau \oplus 1 \oplus \tau = 1 \oplus 2 \cdot \tau$$

Thus, fusing three anyons will yield a final state of total charge τ in 2 ways, or a charge of 1 in exactly one way. We use three states to define our basis.[20] However, because we wish to encode these three anyon states as superpositions of 0 and 1, we need to limit the basis to a two-dimensional Hilbert space. Thus, we consider only two states with a total charge of τ. This choice is purely phenomenological. In these states, we group the two leftmost anyons into a 'control group', and leave the rightmost as a 'non-

computational anyon'. We classify a $|0\rangle$ state as one where the control group has total 'fused' charge of $\mathbf{1}$, and a state of $|1\rangle$ has a control group with a total 'fused' charge of $\boldsymbol{\tau}$. For a more complete description, see Nayak.[20]

Gates

Following the ideas above, adiabatically braiding these anyons around each-other will result in a unitary transformation. These braid operators are a result of two subclasses of operators:

- The *F* matrix
- The *R* matrix

The *R* matrix can be conceptually thought of as the topological phase that is imparted onto the anyons during the braid. As the anyons wind around each-other, they pick up some phase due to the Aharonov–Bohm effect.

The *F* matrix is a result of the physical rotations of the anyons. As they braid between each-other, it is important to realize that the bottom two anyons—the control group—will still distinguish the state of the qubit. Thus, braiding the anyons will change which anyons are in the control group, and therefore change the basis. We evaluate the anyons by always fusing the control group (the bottom anyons) together first, so exchanging which anyons these are will rotate the system. Because these anyons are non-abelian, the order of the anyons (which ones are within the control group) will matter, and as such they will transform the system.

The complete braid operator can be derived as:

$$B = F^{-1}RF$$

In order to mathematically construct the *F* and *R* operators, we can consider permutations of these F and R operators. We know that if we sequentially change the basis that we are operating on, this will eventually lead us back to the same basis. Similarly, we know that if we braid anyons around each-other a certain number of times, this will lead back to the same state. These axioms are called the pentagonal and hexagonal axioms respectively as performing the operation can be visualized with a pentagon/hexagon of state transformations. Although mathematically difficult,[21] these can be approached much more successfully visually.

With these braid operators, we can finally formalize the notion of braids in terms of how they act on our Hilbert space and construct arbitrary universal quantum gates.[22]

See also

- Topological order
- Symmetry-protected topological order
- Ginzburg–Landau theory
- Husimi Q representation

- Random matrix

References

1. Kitaev, Alexei (9 July 1997). "Fault-tolerant quantum computation by anyons". *Annals of Physics*. **303** (1): 2–30. arXiv:quant-ph/9707021v1 (https://arxiv.org/abs/quant-ph/9707021v1). Bibcode:2003AnPhy.303....2K (https://ui.adsabs.harvard.edu/abs/2003AnPhy.303....2K). doi:10.1016/S0003-4916(02)00018-0 (https://doi.org/10.1016%2FS0003-4916%2802%2900018-0). S2CID 11199664 (https://api.semanticscholar.org/CorpusID:11199664).
2. Pires, Francisco (20 March 2022). "Microsoft Chooses Exotic "Topological Qubits" as Future of Quantum Computing" (https://www.tomshardware.com/news/microsoft-chooses-exotic-topological-qubits-as-future-of-quantum-computing). *Tom's Hardware*. Retrieved 1 July 2024.
3. Gibney, Elizabeth (21 October 2016). "Inside Microsoft's quest for a topological quantum computer" (https://www.nature.com/articles/nature.2016.20774). *Nature*. Retrieved 1 July 2024.
4. Aghaee, Morteza (21 June 2023). "InAs-Al hybrid devices passing the topological gap protocol". *Phys. Rev. B*. **107** (24): 245423. arXiv:2207.02472 (https://arxiv.org/abs/2207.02472). Bibcode:2023PhRvB.107x5423A (https://ui.adsabs.harvard.edu/abs/2023PhRvB.107x5423A). doi:10.1103/PhysRevB.107.245423 (https://doi.org/10.1103%2FPhysRevB.107.245423).
5. Yirka, Bob (24 June 2023). "Microsoft claims to have achieved first milestone in creating a reliable and practical quantum computer" (https://phys.org/news/2023-06-microsoft-milestone-reliable-quantum.html#google_vignette). *Phys.org*. Retrieved 1 July 2024.
6. Castelvecchi, Davide (July 3, 2020). "Welcome anyons! Physicists find best evidence yet for long-sought 2D structures" (https://doi.org/10.1038%2Fd41586-020-01988-0). *Nature*. **583** (7815): 176–177. Bibcode:2020Natur.583..176C (https://ui.adsabs.harvard.edu/abs/2020Natur.583..176C). doi:10.1038/d41586-020-01988-0 (https://doi.org/10.1038%2Fd41586-020-01988-0). PMID 32620884 (https://pubmed.ncbi.nlm.nih.gov/32620884). S2CID 220336025 (https://api.semanticscholar.org/CorpusID:220336025). "Simon and others have developed elaborate theories that use anyons as the platform for quantum computers. Pairs of the quasiparticle could encode information in their memory of how they have circled around one another. And because the fractional statistics is 'topological' — it depends on the number of times one anyon went around another, and not on slight changes to its path — it is unaffected by tiny perturbations. This robustness could make topological quantum computers easier to scale up than are current quantum-computing technologies, which are error-prone."
7. Camino, Fernando E.; Zhou, Wei; Goldman, Vladimir J. (December 6, 2005). "Aharonov–Bohm superperiod in a Laughlin quasiparticle interferometer" (https://doi.org/10.1103%2FPhysRevLett.95.246802). *Phys. Rev. Lett*. **95** (24): 246802. arXiv:cond-mat/0504341 (https://arxiv.org/abs/cond-mat/0504341). Bibcode:2005PhRvL..95x6802C (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95x6802C). doi:10.1103/PhysRevLett.95.246802 (https://doi.org/10.1103%2FPhysRevLett.95.246802). PMID 16384405 (https://pubmed.ncbi.nlm.nih.gov/16384405).
8. Willet, R. L. (January 15, 2013). "Magnetic field-tuned Aharonov–Bohm oscillations and evidence for non-Abelian anyons at ν = 5/2". *Physical Review Letters*. **111** (18): 186401. arXiv:1301.2639 (https://arxiv.org/abs/1301.2639). Bibcode:2013PhRvL.111r6401W (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111r6401W). doi:10.1103/PhysRevLett.111.186401 (https://doi.org/10.1103%2FPhysRevLett.111.186401). PMID 24237543 (https://pubmed.ncbi.nlm.nih.gov/24237543). S2CID 22780228 (https://api.semanticscholar.org/CorpusID:22780228).

9. von Keyserling, Curt; Simon, S. H.; Bernd, Rosenow (2015). "Enhanced Bulk-Edge Coulomb Coupling in Fractional Fabry-Perot Interferometers". *Physical Review Letters*. **115** (12): 126807. arXiv:1411.4654 (https://arxiv.org/abs/1411.4654). Bibcode:2015PhRvL.115l6807V (https://ui.adsabs.harvard.edu/abs/2015PhRvL.115l6807V). doi:10.1103/PhysRevLett.115.126807 (https://doi.org/10.1103%2FPhysRevLett.115.126807). PMID 26431008 (https://pubmed.ncbi.nlm.nih.gov/26431008). S2CID 20103218 (https://api.semanticscholar.org/CorpusID:20103218).
10. Ball, Philip (29 September 2021). "Major Quantum Computing Strategy Suffers Serious Setbacks" (https://www.quantamagazine.org/major-quantum-computing-strategy-suffers-serious-setbacks-20210929/). *Quanta Magazine*. Retrieved 30 September 2021.
11. Wood, Charlie (9 May 2023). "Physicists Create Elusive Particles That Remember Their Pasts" (https://www.quantamagazine.org/physicists-create-elusive-particles-that-remember-their-pasts-20230509/). *Quanta Magazine*.
12. Andersen, Trond; et al. (9 October 2023). "Observation of non-Abelian exchange statistics on a superconducting processor". *Bulletin of the American Physical Society*. arXiv:2210.10255 (https://arxiv.org/abs/2210.10255).
13. Iqbal, Mohsin and more (2024). "Non-Abelian topological order and anyons on a trapped-ion processor". *Nature*. **626** (7999): 505–511. arXiv:2305.03766 (https://arxiv.org/abs/2305.03766). Bibcode:2024Natur.626..505I (https://ui.adsabs.harvard.edu/abs/2024Natur.626..505I). doi:10.1038/s41586-023-06934-4 (https://doi.org/10.1038%2Fs41586-023-06934-4). PMID 38356069 (https://pubmed.ncbi.nlm.nih.gov/38356069).
14. Freedman, Michael H.; Larsen, Michael; Wang, Zhenghan (2002-06-01). "A Modular Functor Which is Universal for Quantum Computation". *Communications in Mathematical Physics*. **227** (3): 605–622. arXiv:quant-ph/0001108 (https://arxiv.org/abs/quant-ph/0001108). Bibcode:2002CMaPh.227..605F (https://ui.adsabs.harvard.edu/abs/2002CMaPh.227..605F). doi:10.1007/s002200200645 (https://doi.org/10.1007%2Fs002200200645). ISSN 0010-3616 (https://search.worldcat.org/issn/0010-3616). S2CID 8990600 (https://api.semanticscholar.org/CorpusID:8990600).
15. Freedman, Michael H.; Kitaev, Alexei; Wang, Zhenghan (2002-06-01). "Simulation of Topological Field Theories by Quantum Computers". *Communications in Mathematical Physics*. **227** (3): 587–603. arXiv:quant-ph/0001071 (https://arxiv.org/abs/quant-ph/0001071). Bibcode:2002CMaPh.227..587F (https://ui.adsabs.harvard.edu/abs/2002CMaPh.227..587F). doi:10.1007/s002200200635 (https://doi.org/10.1007%2Fs002200200635). ISSN 0010-3616 (https://search.worldcat.org/issn/0010-3616). S2CID 449219 (https://api.semanticscholar.org/CorpusID:449219).
16. Freedman, Michael; Kitaev, Alexei; Larsen, Michael; Wang, Zhenghan (2003-01-01). "Topological quantum computation" (http://www.ams.org/bull/2003-40-01/S0273-0979-02-00964-3/). *Bulletin of the American Mathematical Society*. **40** (1): 31–38. arXiv:quant-ph/0101025 (https://arxiv.org/abs/quant-ph/0101025). doi:10.1090/S0273-0979-02-00964-3 (https://doi.org/10.1090%2FS0273-0979-02-00964-3). ISSN 0273-0979 (https://search.worldcat.org/issn/0273-0979).
17. Raussendorf, R.; Harrington, J.; Goyal, K. (2007-01-01). "Topological fault-tolerance in cluster state quantum computation". *New Journal of Physics*. **9** (6): 199. arXiv:quant-ph/0703143 (https://arxiv.org/abs/quant-ph/0703143). Bibcode:2007NJPh....9..199R (https://ui.adsabs.harvard.edu/abs/2007NJPh....9..199R). doi:10.1088/1367-2630/9/6/199 (https://doi.org/10.1088%2F1367-2630%2F9%2F6%2F199). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 13811487 (https://api.semanticscholar.org/CorpusID:13811487).
18. Pierce, Cheryl; University, Purdue. "Proposed quantum device may succinctly realize emergent particles such as the Fibonacci anyon" (https://phys.org/news/2023-02-quantum-device-succinctly-emergent-particles.html). *phys.org*. Retrieved 2024-02-25.

19. Trebst, Simon; Troyer, Matthias; Wang, Zhenghan; Ludwig, Andreas W. W. (2008). "A Short Introduction to Fibonacci Anyon Models". *Progress of Theoretical Physics Supplement*. **176**: 384–407. arXiv:0902.3275 (https://arxiv.org/abs/0902.3275). Bibcode:2008PThPS.176..384T (https://ui.adsabs.harvard.edu/abs/2008PThPS.176..384T). doi:10.1143/PTPS.176.384 (https://doi.org/10.1143%2FPTPS.176.384). S2CID 16880657 (https://api.semanticscholar.org/CorpusID:16880657).
20. Nayak, Chetan (2008). "Non-Abelian Anyons and Topological Quantum Computation". *Reviews of Modern Physics*. **80** (3): 1083–1159. arXiv:0707.1889 (https://arxiv.org/abs/0707.1889). Bibcode:2008RvMP...80.1083N (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1083N). doi:10.1103/RevModPhys.80.1083 (https://doi.org/10.1103%2FRevModPhys.80.1083). S2CID 119628297 (https://api.semanticscholar.org/CorpusID:119628297).
21. Eric Paquette. Topological quantum computing with anyons, 2009. Categories, Logic and Foundations of Physics IV.
22. Explicit braids that perform particular quantum computations with Fibonacci anyons have been given by Bonesteel, N. E.; Hormozi, L.; Zikos, G.; Simon, S. H.; West, K. W. (2005). "Braid Topologies for Quantum Computation". *Physical Review Letters*. **95** (14): 140503. arXiv:quant-ph/0505065 (https://arxiv.org/abs/quant-ph/0505065). Bibcode:2005PhRvL..95n0503B (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95n0503B). doi:10.1103/PhysRevLett.95.140503 (https://doi.org/10.1103%2FPhysRevLett.95.140503). PMID 16241636 (https://pubmed.ncbi.nlm.nih.gov/16241636). S2CID 1246885 (https://api.semanticscholar.org/CorpusID:1246885).

Further reading

- Collins, Graham P. (April 2006). "Computing with Quantum Knots" (http://www.cs.virginia.edu/~robins/Computing_with_Quantum_Knots.pdf) (PDF). *Scientific American*.
- Sarma, Sankar Das; Freedman, Michael; Nayak, Chetan (2005). "Topologically Protected Qubits from a Possible Non-Abelian Fractional Quantum Hall State". *Physical Review Letters*. **94** (16): 166802. arXiv:cond-mat/0412343 (https://arxiv.org/abs/cond-mat/0412343). Bibcode:2005PhRvL..94p6802D (https://ui.adsabs.harvard.edu/abs/2005PhRvL..94p6802D). doi:10.1103/PhysRevLett.94.166802 (https://doi.org/10.1103%2FPhysRevLett.94.166802). PMID 15904258 (https://pubmed.ncbi.nlm.nih.gov/15904258). S2CID 8773427 (https://api.semanticscholar.org/CorpusID:8773427).
- Nayak, Chetan; Simon, Steven H.; Stern, Ady; Freedman, Michael; Sarma, Sankar Das (2008). "Non-Abelian Anyons and Topological Quantum Computation". *Reviews of Modern Physics*. **80** (3): 1083–1159. arXiv:0707.1889 (https://arxiv.org/abs/0707.1889). Bibcode:2008RvMP...80.1083N (https://ui.adsabs.harvard.edu/abs/2008RvMP...80.1083N). doi:10.1103/RevModPhys.80.1083 (https://doi.org/10.1103%2FRevModPhys.80.1083). S2CID 119628297 (https://api.semanticscholar.org/CorpusID:119628297).
- Simon, Steven H. "Quantum Computing with a Twist" (http://physicsworld.com/cws/article/indepth/43623).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Topological_quantum_computer&oldid=1232515352"

WIKIPEDIA
The Free Encyclopedia

Quantum error correction

Quantum error correction (**QEC**) is a set of techniques used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction is theorised as essential to achieve fault tolerant quantum computing that can reduce the effects of noise on stored quantum information, faulty quantum gates, faulty quantum state preparation, and faulty measurements. Effective quantum error correction would allow quantum computers with low qubit fidelity to execute algorithms of higher complexity or greater circuit depth.[1]

Classical error correction often employs redundancy. The simplest albeit inefficient approach is the repetition code. A repetition code stores the desired (logical) information as multiple copies, and—if these copies are later found to disagree due to errors introduced to the system-determines the most likely value for the original data by majority vote. E.g. suppose we copy a bit in the one (on) state three times. Suppose further that noise in the system introduces an error which corrupts the three-bit state so that one of the copied bits becomes zero (off) but the other two remain equal to one. Assuming that errors are independent and occur with some sufficiently low probability *p*, it is most likely that the error is a single-bit error and the intended message is three bits in the one state. It is possible that a double-bit error occurs and the transmitted message is equal to three zeros, but this outcome is less likely than the above outcome. In this example, the logical information is a single bit in the one state and the physical information are the three duplicate bits. Creating a physical state that represents the logical state is called *encoding* and determining which logical state is encoded in the physical state is called *decoding*. Similar to classical error correction, QEC codes do not always correctly decode logical qubits, but instead reduce the effect of noise on the logical state.

Copying quantum information is not possible due to the no-cloning theorem. This theorem seems to present an obstacle to formulating a theory of quantum error correction. But it is possible to *spread* the (logical) information of one logical qubit onto a highly entangled state of several (physical) qubits. Peter Shor first discovered this method of formulating a *quantum error correcting code* by storing the information of one qubit onto a highly entangled state of nine qubits.[2]

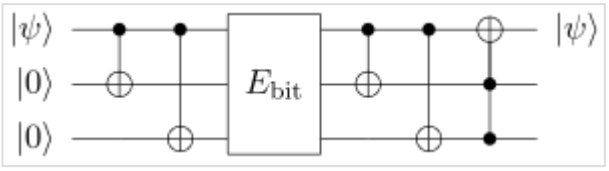
In classical error correction, *syndrome decoding* is used to diagnose which error was the likely source of corruption on an encoded state. An error can then be reversed by applying a corrective operation based on the syndrome. Quantum error correction also employs syndrome measurements. It performs a multi-qubit measurement that does not disturb the quantum information in the encoded state but retrieves information about the error. Depending on the QEC code used, syndrome measurement can determine the occurrence, location and type of errors. In most QEC codes, the type of error is either a bit flip, or a sign (of the phase) flip, or both (corresponding to the Pauli matrices X, Z, and Y). The measurement of the syndrome has the projective effect of a quantum measurement, so even if the error due to the noise was arbitrary, it can be expressed as a combination of basis operations called the error basis (which is given by the Pauli matrices and the identity). To correct the error, the Pauli operator corresponding to the type of error is used on the corrupted qubit to revert the effect of the error.

The syndrome measurement provides information about the error that has happened, but not about the information that is stored in the logical qubit—as otherwise the measurement would destroy any quantum superposition of this logical qubit with other qubits in the quantum computer, which would prevent it from being used to convey quantum information.

Bit flip code

The repetition code works in a classical channel, because classical bits are easy to measure and to repeat. This approach does not work for a quantum channel in which, due to the no-cloning theorem, it is not possible to repeat a single qubit three times. To overcome this, a different method has to be used, such as the *three-qubit bit flip code* first proposed by Asher Peres in 1985.[3] This technique uses entanglement and syndrome measurements and is comparable in performance with the repetition code.

Consider the situation in which we want to transmit the state of a single qubit $|\psi\rangle$ through a noisy channel $\mathcal{E}$. Let us moreover assume that this channel either flips the state of the qubit, with probability p, or leaves it unchanged. The action of $\mathcal{E}$ on a general input ρ can therefore be written as $\mathcal{E}(\rho) = (1-p)\rho + p\, X\rho X$.



Quantum circuit of the bit flip code

Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ be the quantum state to be transmitted. With no error correcting protocol in place, the transmitted state will be correctly transmitted with probability $1-p$. We can however improve on this number by *encoding* the state into a greater number of qubits, in such a way that errors in the corresponding logical qubits can be detected and corrected. In the case of the simple three-qubit repetition code, the encoding consists in the mappings $|0\rangle \to |0_{\mathrm{L}}\rangle \equiv |000\rangle$ and $|1\rangle \to |1_{\mathrm{L}}\rangle \equiv |111\rangle$. The input state $|\psi\rangle$ is encoded into the state $|\psi'\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$. This mapping can be realized for example using two CNOT gates, entangling the system with two ancillary qubits initialized in the state $|0\rangle$.[4] The encoded state $|\psi'\rangle$ is what is now passed through the noisy channel.

The channel acts on $|\psi'\rangle$ by flipping some subset (possibly empty) of its qubits. No qubit is flipped with probability $(1-p)^3$, a single qubit is flipped with probability $3p(1-p)^2$, two qubits are flipped with probability $3p^2(1-p)$, and all three qubits are flipped with probability p^3. Note that a further assumption about the channel is made here: we assume that $\mathcal{E}$ acts equally and independently on each of the three qubits in which the state is now encoded. The problem is now how to detect and correct such errors, while not corrupting the transmitted state.

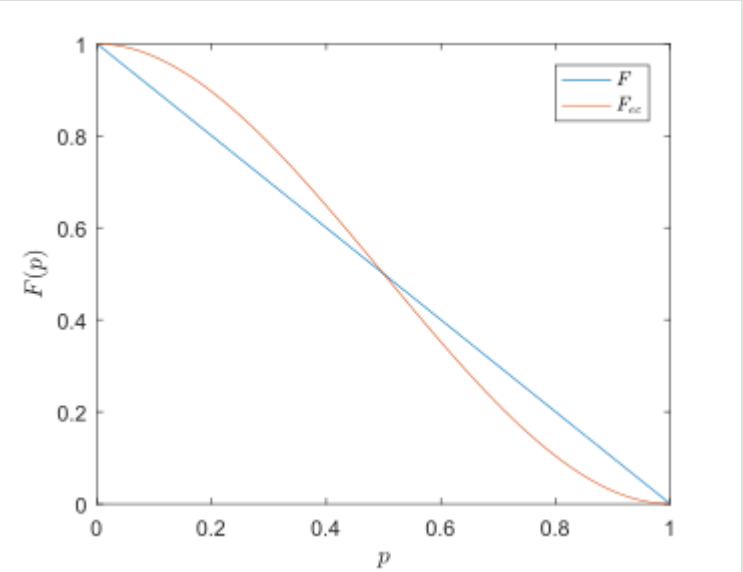
Let us assume for simplicity that p is small enough that the probability of more than a single qubit being flipped is negligible. One can then detect whether a qubit was flipped, without also querying for the values being transmitted, by asking whether one of the qubits differs from the others. This amounts to

performing a measurement with four different outcomes, corresponding to the following four projective measurements:

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|, \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned}$$

This reveals which qubits are different from the others, without at the same time giving information about the state of the qubits themselves. If the outcome corresponding to P_0 is obtained, no correction is applied, while if the outcome corresponding to P_i is observed, then the Pauli X gate is applied to the i-th qubit. Formally, this correcting procedure corresponds to the application of the following map to the output of the channel:

$$\mathcal{E}_{\text{corr}}(\rho) = P_0 \rho P_0 + \sum_{i=1}^{3} X_i P_i \rho P_i X_i.$$



Comparison of output *minimum* fidelities, with (red) and without (blue) error correcting via the three qubit bit flip code. Notice how, for $p \leq 1/2$, the error correction scheme improves the fidelity.

Note that, while this procedure perfectly corrects the output when zero or one flips are introduced by the channel, if more than one qubit is flipped then the output is not properly corrected. For example, if the first and second qubits are flipped, then the syndrome measurement gives the outcome P_3, and the third qubit is flipped, instead of the first two. To assess the performance of this error-correcting scheme for a general input we can study the fidelity $F(\psi')$ between the input $|\psi'\rangle$ and the output $\rho_{\text{out}} \equiv \mathcal{E}_{\text{corr}}(\mathcal{E}(|\psi'\rangle\langle\psi'|))$. Being the output state ρ_{out} correct when no more than one qubit is flipped, which happens with probability $(1-p)^3 + 3p(1-p)^2$, we can write it as $[(1-p)^3 + 3p(1-p)^2]\,|\psi'\rangle\langle\psi'| + (\dots)$, where the dots denote components of ρ_{out} resulting from errors not properly corrected by the protocol. It follows that

$$F(\psi') = \langle\psi'|\rho_{\text{out}}|\psi'\rangle \geq (1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3.$$

This fidelity is to be compared with the corresponding fidelity obtained when no error-correcting protocol is used, which was shown before to equal $1-p$. A little algebra then shows that the fidelity *after* error correction is greater than the one without for $p < 1/2$. Note that this is consistent with the working assumption that was made while deriving the protocol (of p being small enough).

Sign flip code

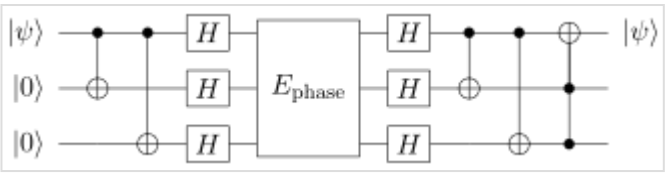
Flipped bits are the only kind of error in classical computer, but there is another possibility of an error with quantum computers, the sign flip. Through the transmission in a channel the relative sign between $|0\rangle$ and $|1\rangle$ can become inverted. For instance, a qubit in the state $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ may have its sign flip to $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

The original state of the qubit

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

will be changed into the state

$$|\psi'\rangle = \alpha_0|{+}{+}{+}\rangle + \alpha_1|{-}{-}{-}\rangle.$$



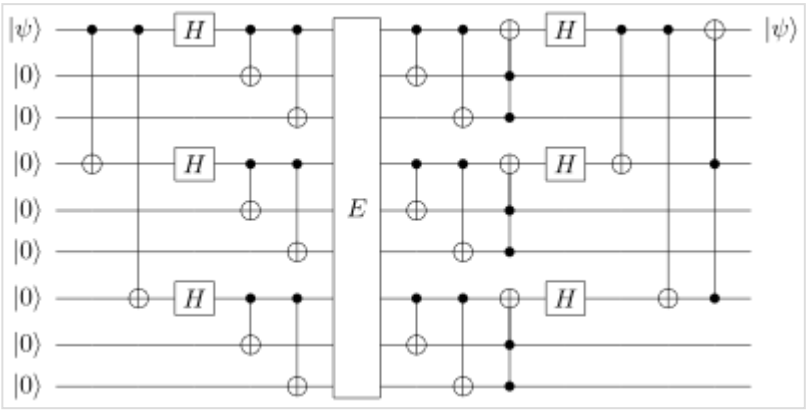
Quantum circuit of the phase flip code

In the Hadamard basis, bit flips become sign flips and sign flips become bit flips. Let $\boldsymbol{E_{\text{phase}}}$ be a quantum channel that can cause at most one phase flip. Then the bit flip code from above can recover $|\psi\rangle$ by transforming into the Hadamard basis before and after transmission through $\boldsymbol{E_{\text{phase}}}$.

Shor code

The error channel may induce either a bit flip, a sign flip (i.e., a phase flip), or both. It is possible to correct for both types of errors on a logical qubit using a well-designed QEC code. One example of a code that does this is the Shor code, published in 1995.[2][5]:10 Since these two types of errors are the only types of errors that can result after a projective measurement, a Shor code corrects arbitrary single-qubit errors.

Let $\boldsymbol{E}$ be a quantum channel that can arbitrarily corrupt a single qubit. The 1st, 4th and 7th qubits are for the sign flip code, while the three groups of qubits (1,2,3), (4,5,6), and (7,8,9) are designed for the bit flip code. With the Shor code, a qubit state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ will be transformed into the product of 9 qubits $|\psi'\rangle = \alpha_0|0_S\rangle + \alpha_1|1_S\rangle$, where



Quantum circuit to encode a single logical qubit with the Shor code and then perform bit flip error correction on each of the three blocks.

$$|0_S\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1_S\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

If a bit flip error happens to a qubit, the syndrome analysis will be performed on each block of qubits (1,2,3), (4,5,6), and (7,8,9) to detect and correct at most one bit flip error in each block.

If the three bit flip group (1,2,3), (4,5,6), and (7,8,9) are considered as three inputs, then the Shor code circuit can be reduced as a sign flip code. This means that the Shor code can also repair a sign flip error for a single qubit.

The Shor code also can correct for any arbitrary errors (both bit flip and sign flip) to a single qubit. If an error is modeled by a unitary transform U, which will act on a qubit $|\psi\rangle$, then U can be described in the form

$$U = c_0 I + c_1 X + c_2 Y + c_3 Z$$

where c_0,c_1,c_2, and c_3 are complex constants, I is the identity, and the Pauli matrices are given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix};$$
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If *U* is equal to *I*, then no error occurs. If $U = X$, a bit flip error occurs. If $U = Z$, a sign flip error occurs. If $U = iY$ then both a bit flip error and a sign flip error occur. In other words, the Shor code can correct any combination of bit or phase errors on a single qubit.

Bosonic codes

Several proposals have been made for storing error-correctable quantum information in bosonic modes. Unlike a two-level system, a quantum harmonic oscillator has infinitely many energy levels in a single physical system. Codes for these systems include cat,[6][7][8] Gottesman-Kitaev-Preskill (GKP),[9] and binomial codes.[10][11] One insight offered by these codes is to take advantage of the redundancy within a single system, rather than to duplicate many two-level qubits.

Binomial code[10]

Written in the Fock basis, the simplest binomial encoding is

$$|0_\mathrm{L}\rangle = \frac{|0\rangle + |4\rangle}{\sqrt{2}}, \quad |1_\mathrm{L}\rangle = |2\rangle,$$

where the subscript L indicates a "logically encoded" state. Then if the dominant error mechanism of the system is the stochastic application of the bosonic lowering operator $\hat{a}$, the corresponding error states are $|3\rangle$ and $|1\rangle$, respectively. Since the codewords involve only even photon number, and the error states involve only odd photon number, errors can be detected by measuring the photon number parity of the system.[10][12] Measuring the odd parity will allow correction by application of an appropriate unitary operation without knowledge of the specific logical state of the qubit. However, the particular binomial code above is not robust to two-photon loss.

Cat code[6][7][8]

Schrödinger cat states, superpositions of coherent states, can also be used as logical states for error correction codes. Cat code, realized by Ofek et al.[13] in 2016, defined two sets of logical states: $\{|0_L^+\rangle, |1_L^+\rangle\}$ and $\{|0_L^-\rangle, |1_L^-\rangle\}$, where each of the states is a superposition of coherent state as follows

$$
\begin{aligned}
|0_L^+\rangle &\equiv |\alpha\rangle + |-\alpha\rangle, \\
|1_L^+\rangle &\equiv |i\alpha\rangle + |-i\alpha\rangle, \\
|0_L^-\rangle &\equiv |\alpha\rangle - |-\alpha\rangle, \\
|1_L^-\rangle &\equiv |i\alpha\rangle - |-i\alpha\rangle.
\end{aligned}
$$

Those two sets of states differ from the photon number parity, as states denoted with $^+$ only occupy even photon number states and states with $^-$ indicate they have odd parity. Similar to the binomial code, if the dominant error mechanism of the system is the stochastic application of the bosonic lowering operator $\hat{a}$, the error takes the logical states from the even parity subspace to the odd one, and vice versa. Single-photon-loss errors can therefore be detected by measuring the photon number parity operator $\exp(i\pi\hat{a}^\dagger\hat{a})$ using a dispersively coupled ancillary qubit.[12]

Still, cat qubits are not protected against two-photon loss $\hat{a}^2$, dephasing noise $\hat{a}^\dagger\hat{a}$, photon-gain error $\hat{a}^\dagger$, etc.

General codes

In general, a *quantum code* for a quantum channel $\mathcal{E}$ is a subspace $\mathcal{C} \subseteq \mathcal{H}$, where $\mathcal{H}$ is the state Hilbert space, such that there exists another quantum channel $\mathcal{R}$ with

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho = P_{\mathcal{C}} \rho P_{\mathcal{C}},$$

where $P_{\mathcal{C}}$ is the orthogonal projection onto $\mathcal{C}$. Here $\mathcal{R}$ is known as the *correction operation*.

A *non-degenerate code* is one for which different elements of the set of correctable errors produce linearly independent results when applied to elements of the code. If distinct of the set of correctable errors produce orthogonal results, the code is considered *pure*.[14]

Models

Over time, researchers have come up with several codes:

- Peter Shor's 9-qubit-code, a.k.a. the Shor code, encodes 1 logical qubit in 9 physical qubits and can correct for arbitrary errors in a single qubit.
- Andrew Steane found a code that does the same with 7 instead of 9 qubits, see Steane code.
- Raymond Laflamme and collaborators found a class of 5-qubit codes that do the same, which also have the property of being fault-tolerant. A 5-qubit code is the smallest possible code that protects a single logical qubit against single-qubit errors.
- A generalisation of the technique used by Steane, to develop the 7-qubit code from the classical [7, 4] Hamming code, led to the construction of an important class of codes called the CSS codes, named for their inventors: Robert Calderbank, Peter Shor and Andrew Steane. According to the quantum Hamming bound, encoding a single logical qubit and providing for arbitrary error correction in a single qubit requires a minimum of 5 physical qubits.
- A more general class of codes (encompassing the former) are the stabilizer codes discovered by Daniel Gottesman, and by Robert Calderbank, Eric Rains, Peter Shor, and N. J. A. Sloane; these are also called additive codes.

- Two dimensional Bacon–Shor codes are a family of codes parameterized by integers *m* and *n*. There are *nm* qubits arranged in a square lattice.[15]
- Alexei Kitaev's topological quantum codes, introduced in 1997 as the toric code, and the more general idea of a topological quantum computer are the basis for various code types.[16]
- Todd Brun, Igor Devetak, and Min-Hsiu Hsieh also constructed the entanglement-assisted stabilizer formalism as an extension of the standard stabilizer formalism that incorporates quantum entanglement shared between a sender and a receiver.
- The ideas of stabilizer codes, CSS codes, and topological codes can be expanded into the 2D planar surface code, of which various types exist.[17] As of June 2024, the 2D planar surface code is generally considered the most well-studied type of quantum error correction, and one of the leading contenders for practical use in quantum computing. [18][19]

That these codes allow indeed for quantum computations of arbitrary length is the content of the quantum threshold theorem, found by Michael Ben-Or and Dorit Aharonov, which asserts that you can correct for all errors if you concatenate quantum codes such as the CSS codes—i.e. re-encode each logical qubit by the same code again, and so on, on logarithmically many levels—*provided* that the error rate of individual quantum gates is below a certain threshold; as otherwise, the attempts to measure the syndrome and correct the errors would introduce more new errors than they correct for.

As of late 2004, estimates for this threshold indicate that it could be as high as 1–3%,[20] provided that there are sufficiently many qubits available.

Experimental realization

There have been several experimental realizations of CSS-based codes. The first demonstration was with nuclear magnetic resonance qubits.[21] Subsequently, demonstrations have been made with linear optics,[22] trapped ions,[23][24] and superconducting (transmon) qubits.[25]

In 2016 for the first time the lifetime of a quantum bit was prolonged by employing a QEC code.[13] The error-correction demonstration was performed on Schrodinger-cat states encoded in a superconducting resonator, and employed a quantum controller capable of performing real-time feedback operations including read-out of the quantum information, its analysis, and the correction of its detected errors. The work demonstrated how the quantum-error-corrected system reaches the break-even point at which the lifetime of a logical qubit exceeds the lifetime of the underlying constituents of the system (the physical qubits).

Other error correcting codes have also been implemented, such as one aimed at correcting for photon loss, the dominant error source in photonic qubit schemes.[26][27]

In 2021, an entangling gate between two logical qubits encoded in topological quantum error-correction codes has first been realized using 10 ions in a trapped-ion quantum computer.[28][29] 2021 also saw the first experimental demonstration of fault-tolerant Bacon-Shor code in a single logical qubit of a trapped-ion system, i.e. a demonstration for which the addition of error correction is able to suppress more errors than is introduced by the overhead required to implement the error correction as well as fault tolerant Steane code.[30][31][32]

In 2022, researchers at the University of Innsbruck have demonstrated a fault-tolerant universal set of gates on two logical qubits in a trapped-ion quantum computer. They have performed a logical two-qubit controlled-NOT gate between two instances of the seven-qubit colour code, and fault-tolerantly prepared a logical magic state.[33]

In February 2023 researchers at Google claimed to have decreased quantum errors by increasing the qubit number in experiments, they used a fault tolerant surface code measuring an error rate of 3.028% and 2.914% for a distance-3 qubit array and a distance-5 qubit array respectively.[34][35][36]

In April 2024, researchers at Microsoft claimed to have successfully tested a quantum error correction code that allowed them to achieve an error rate with logical qubits that is 800 times better than the underlying physical error rate.[37]

This qubit virtualization system was used to create 4 logical qubits with 30 of the 32 qubits on Quantinuum's trapped-ion hardware. The system uses an active syndrome extraction technique to diagnose errors and correct them while calculations are underway without destroying the logical qubits.[38]

Quantum error-correction without encoding and parity-checks

In 2022, research at University of Engineering and Technology Lahore demonstrated error-cancellation by inserting single-qubit Z-axis rotation gates into strategically chosen locations of the superconductor quantum circuits.[39] The scheme has been shown to effectively correct errors that would otherwise rapidly add up under constructive interference of coherent noise. This is a circuit-level calibration scheme that traces deviations (e.g. sharp dips or notches) in the decoherence curve to detect and localize the coherent error, but does not require encoding or parity measurements.[40] However, further investigation is needed to establish the effectiveness of this method for the incoherent noise.[39]

See also

- Error detection and correction
- Soft error

References

1. Cai, Weizhou; Ma, Yuwei (2021). "Bosonic quantum error correction codes in superconducting quantum circuits" (https://doi.org/10.1016%2Fj.fmre.2020.12.006). *Fundamental Research*. **1** (1): 50–67. arXiv:2010.08699 (https://arxiv.org/abs/2010.08699). Bibcode:2021FunRe...1...50C (https://ui.adsabs.harvard.edu/abs/2021FunRe...1...50C). doi:10.1016/j.fmre.2020.12.006 (https://doi.org/10.1016%2Fj.fmre.2020.12.006). "A practical quantum computer that is capable of large circuit depth, therefore, ultimately calls for operations on logical qubits protected by quantum error correction"

2. Shor, Peter W. (1995). "Scheme for reducing decoherence in quantum computer memory". *Physical Review A*. **52** (4): R2493–R2496. Bibcode:1995PhRvA..52.2493S (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.2493S). doi:10.1103/PhysRevA.52.R2493 (https://doi.org/10.1103%2FPhysRevA.52.R2493). PMID 9912632 (https://pubmed.ncbi.nlm.nih.gov/9912632).
3. Peres, Asher (1985). "Reversible Logic and Quantum Computers". *Physical Review A*. **32** (6): 3266–3276. Bibcode:1985PhRvA..32.3266P (https://ui.adsabs.harvard.edu/abs/1985PhRvA..32.3266P). doi:10.1103/PhysRevA.32.3266 (https://doi.org/10.1103%2FPhysRevA.32.3266). PMID 9896493 (https://pubmed.ncbi.nlm.nih.gov/9896493).
4. Nielsen, Michael A.; Chuang, Isaac L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.
5. Devitt, Simon J; Munro, William J; Nemoto, Kae (2013-06-20). "Quantum error correction for beginners" (https://dx.doi.org/10.1088/0034-4885/76/7/076001). *Reports on Progress in Physics*. **76** (7): 076001. arXiv:0905.2794 (https://arxiv.org/abs/0905.2794). Bibcode:2013RPPh...76g6001D (https://ui.adsabs.harvard.edu/abs/2013RPPh...76g6001D). doi:10.1088/0034-4885/76/7/076001 (https://doi.org/10.1088%2F0034-4885%2F76%2F7%2F076001). ISSN 0034-4885 (https://search.worldcat.org/issn/0034-4885). PMID 23787909 (https://pubmed.ncbi.nlm.nih.gov/23787909). S2CID 206021660 (https://api.semanticscholar.org/CorpusID:206021660).
6. Cochrane, P. T.; Milburn, G. J.; Munro, W. J. (1999-04-01). "Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping". *Physical Review A*. **59** (4): 2631–2634. arXiv:quant-ph/9809037 (https://arxiv.org/abs/quant-ph/9809037). Bibcode:1999PhRvA..59.2631C (https://ui.adsabs.harvard.edu/abs/1999PhRvA..59.2631C). doi:10.1103/PhysRevA.59.2631 (https://doi.org/10.1103%2FPhysRevA.59.2631). S2CID 119532538 (https://api.semanticscholar.org/CorpusID:119532538).
7. Leghtas, Zaki; Kirchmair, Gerhard; Vlastakis, Brian; Schoelkopf, Robert J.; Devoret, Michel H.; Mirrahimi, Mazyar (2013-09-20). "Hardware-Efficient Autonomous Quantum Memory Protection". *Physical Review Letters*. **111** (12): 120501. arXiv:1207.0679 (https://arxiv.org/abs/1207.0679). Bibcode:2013PhRvL.111l0501L (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111l0501L). doi:10.1103/physrevlett.111.120501 (https://doi.org/10.1103%2Fphysrevlett.111.120501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 24093235 (https://pubmed.ncbi.nlm.nih.gov/24093235). S2CID 19929020 (https://api.semanticscholar.org/CorpusID:19929020).
8. Mirrahimi, Mazyar; Leghtas, Zaki; Albert, Victor V; Touzard, Steven; Schoelkopf, Robert J; Jiang, Liang; Devoret, Michel H (2014-04-22). "Dynamically protected cat-qubits: a new paradigm for universal quantum computation". *New Journal of Physics*. **16** (4): 045014. arXiv:1312.2017 (https://arxiv.org/abs/1312.2017). Bibcode:2014NJPh...16d5014M (https://ui.adsabs.harvard.edu/abs/2014NJPh...16d5014M). doi:10.1088/1367-2630/16/4/045014 (https://doi.org/10.1088%2F1367-2630%2F16%2F4%2F045014). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 7179816 (https://api.semanticscholar.org/CorpusID:7179816).
9. Daniel Gottesman; Alexei Kitaev; John Preskill (2001). "Encoding a qubit in an oscillator". *Physical Review A*. **64** (1): 012310. arXiv:quant-ph/0008040 (https://arxiv.org/abs/quant-ph/0008040). Bibcode:2001PhRvA..64a2310G (https://ui.adsabs.harvard.edu/abs/2001PhRvA..64a2310G). doi:10.1103/PhysRevA.64.012310 (https://doi.org/10.1103%2FPhysRevA.64.012310). S2CID 18995200 (https://api.semanticscholar.org/CorpusID:18995200).
10. Michael, Marios H.; Silveri, Matti; Brierley, R. T.; Albert, Victor V.; Salmilehto, Juha; Jiang, Liang; Girvin, S. M. (2016-07-14). "New Class of Quantum Error-Correcting Codes for a Bosonic Mode". *Physical Review X*. **6** (3): 031006. arXiv:1602.00008 (https://arxiv.org/abs/1602.00008). Bibcode:2016PhRvX...6c1006M (https://ui.adsabs.harvard.edu/abs/2016PhRvX...6c1006M). doi:10.1103/PhysRevX.6.031006 (https://doi.org/10.1103%2FPhysRevX.6.031006). S2CID 29518512 (https://api.semanticscholar.org/CorpusID:29518512).

11. Albert, Victor V.; Noh, Kyungjoo; Duivenvoorden, Kasper; Young, Dylan J.; Brierley, R. T.; Reinhold, Philip; Vuillot, Christophe; Li, Linshu; Shen, Chao; Girvin, S. M.; Terhal, Barbara M.; Jiang, Liang (2018). "Performance and structure of single-mode bosonic codes". *Physical Review A*. **97** (3): 032346. arXiv:1708.05010 (https://arxiv.org/abs/1708.05010). Bibcode:2018PhRvA..97c2346A (https://ui.adsabs.harvard.edu/abs/2018PhRvA..97c2346A). doi:10.1103/PhysRevA.97.032346 (https://doi.org/10.1103%2FPhysRevA.97.032346). S2CID 51691343 (https://api.semanticscholar.org/CorpusID:51691343).
12. Sun, L.; Petrenko, A.; Leghtas, Z.; Vlastakis, B.; Kirchmair, G.; Sliwa, K. M.; Narla, A.; Hatridge, M.; Shankar, S.; Blumoff, J.; Frunzio, L.; Mirrahimi, M.; Devoret, M. H.; Schoelkopf, R. J. (July 2014). "Tracking photon jumps with repeated quantum non-demolition parity measurements". *Nature*. **511** (7510): 444–448. arXiv:1311.2534 (https://arxiv.org/abs/1311.2534). Bibcode:2014Natur.511..444S (https://ui.adsabs.harvard.edu/abs/2014Natur.511..444S). doi:10.1038/nature13436 (https://doi.org/10.1038%2Fnature13436). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 25043007 (https://pubmed.ncbi.nlm.nih.gov/25043007). S2CID 987945 (https://api.semanticscholar.org/CorpusID:987945).
13. Ofek, Nissim; Petrenko, Andrei; Heeres, Reinier; Reinhold, Philip; Leghtas, Zaki; Vlastakis, Brian; Liu, Yehan; Frunzio, Luigi; Girvin, S. M.; Jiang, L.; Mirrahimi, Mazyar (August 2016). "Extending the lifetime of a quantum bit with error correction in superconducting circuits". *Nature*. **536** (7617): 441–445. Bibcode:2016Natur.536..441O (https://ui.adsabs.harvard.edu/abs/2016Natur.536..441O). doi:10.1038/nature18949 (https://doi.org/10.1038%2Fnature18949). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 27437573 (https://pubmed.ncbi.nlm.nih.gov/27437573). S2CID 594116 (https://api.semanticscholar.org/CorpusID:594116).
14. Calderbank, A. R.; Rains, E. M.; Shor, P. W.; Sloane, N. J. A. (1998). "Quantum Error Correction via Codes over GF(4)". *IEEE Transactions on Information Theory*. **44** (4): 1369–1387. arXiv:quant-ph/9608006 (https://arxiv.org/abs/quant-ph/9608006). doi:10.1109/18.681315 (https://doi.org/10.1109%2F18.681315). S2CID 1215697 (https://api.semanticscholar.org/CorpusID:1215697).
15. Bacon, Dave (2006-01-30). "Operator quantum error-correcting subsystems for self-correcting quantum memories". *Physical Review A*. **73** (1): 012340. arXiv:quant-ph/0506023 (https://arxiv.org/abs/quant-ph/0506023). Bibcode:2006PhRvA..73a2340B (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73a2340B). doi:10.1103/PhysRevA.73.012340 (https://doi.org/10.1103%2FPhysRevA.73.012340). S2CID 118968017 (https://api.semanticscholar.org/CorpusID:118968017).
16. Kitaev, Alexei (1997-07-31). "Quantum Error Correction with Imperfect Gates" (https://link.springer.com/book/10.1007/978-1-4615-5923-8). *Quantum Communication, Computing, and Measurement*. Springer. pp. 181–188. doi:10.1007/978-1-4615-5923-8 (https://doi.org/10.1007%2F978-1-4615-5923-8).
17. Fowler, Austin G.; Mariantoni, Matteo; Martinis, John M.; Cleland, Andrew N. (2012-09-18). "Surface codes: Towards practical large-scale quantum computation". *Physical Review A*. **86** (3): 032324. arXiv:1208.0928 (https://arxiv.org/abs/1208.0928). Bibcode:2012PhRvA..86c2324F (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86c2324F). doi:10.1103/PhysRevA.86.032324 (https://doi.org/10.1103%2FPhysRevA.86.032324). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947).
18. Gidney, Craig; Newman, Michael; Brooks, Peter; Jones, Cody (2023). "Yoked surface codes". arXiv:2312.04522 (https://arxiv.org/abs/2312.04522) [quant-ph (https://arxiv.org/archive/quant-ph)].
19. Horsman, Dominic; Fowler, Austin G; Devitt, Simon; Meter, Rodney Van (2012-12-01). "Surface code quantum computing by lattice surgery". *New Journal of Physics*. **14** (12): 123011. arXiv:1111.4022 (https://arxiv.org/abs/1111.4022). Bibcode:2012NJPh...14l3011H (https://ui.adsabs.harvard.edu/abs/2012NJPh...14l3011H). doi:10.1088/1367-2630/14/12/123011 (https://doi.org/10.1088%2F1367-2630%2F14%2F12%2F123011). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).

20. Knill, Emanuel (2004-11-02). "Quantum Computing with Very Noisy Devices". *Nature*. **434** (7029): 39–44. arXiv:quant-ph/0410199 (https://arxiv.org/abs/quant-ph/0410199). Bibcode:2005Natur.434...39K (https://ui.adsabs.harvard.edu/abs/2005Natur.434...39K). doi:10.1038/nature03350 (https://doi.org/10.1038%2Fnature03350). PMID 15744292 (https://pubmed.ncbi.nlm.nih.gov/15744292). S2CID 4420858 (https://api.semanticscholar.org/CorpusID:4420858).
21. Cory, D. G.; Price, M. D.; Maas, W.; Knill, E.; Laflamme, R.; Zurek, W. H.; Havel, T. F.; Somaroo, S. S. (1998). "Experimental Quantum Error Correction". *Phys. Rev. Lett*. **81** (10): 2152–2155. arXiv:quant-ph/9802018 (https://arxiv.org/abs/quant-ph/9802018). Bibcode:1998PhRvL..81.2152C (https://ui.adsabs.harvard.edu/abs/1998PhRvL..81.2152C). doi:10.1103/PhysRevLett.81.2152 (https://doi.org/10.1103%2FPhysRevLett.81.2152). S2CID 11662810 (https://api.semanticscholar.org/CorpusID:11662810).
22. Pittman, T. B.; Jacobs, B. C.; Franson, J. D. (2005). "Demonstration of quantum error correction using linear optics". *Phys. Rev. A*. **71** (5): 052332. arXiv:quant-ph/0502042 (https://arxiv.org/abs/quant-ph/0502042). Bibcode:2005PhRvA..71e2332P (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71e2332P). doi:10.1103/PhysRevA.71.052332 (https://doi.org/10.1103%2FPhysRevA.71.052332). S2CID 11679660 (https://api.semanticscholar.org/CorpusID:11679660).
23. Chiaverini, J.; Leibfried, D.; Schaetz, T.; Barrett, M. D.; Blakestad, R. B.; Britton, J.; Itano, W. M.; Jost, J. D.; Knill, E.; Langer, C.; Ozeri, R.; Wineland, D. J. (2004). "Realization of quantum error correction". *Nature*. **432** (7017): 602–605. Bibcode:2004Natur.432..602C (https://ui.adsabs.harvard.edu/abs/2004Natur.432..602C). doi:10.1038/nature03074 (https://doi.org/10.1038%2Fnature03074). PMID 15577904 (https://pubmed.ncbi.nlm.nih.gov/15577904). S2CID 167898 (https://api.semanticscholar.org/CorpusID:167898).
24. Schindler, P.; Barreiro, J. T.; Monz, T.; Nebendahl, V.; Nigg, D.; Chwalla, M.; Hennrich, M.; Blatt, R. (2011). "Experimental Repetitive Quantum Error Correction". *Science*. **332** (6033): 1059–1061. Bibcode:2011Sci...332.1059S (https://ui.adsabs.harvard.edu/abs/2011Sci...332.1059S). doi:10.1126/science.1203329 (https://doi.org/10.1126%2Fscience.1203329). PMID 21617070 (https://pubmed.ncbi.nlm.nih.gov/21617070). S2CID 32268350 (https://api.semanticscholar.org/CorpusID:32268350).
25. Reed, M. D.; DiCarlo, L.; Nigg, S. E.; Sun, L.; Frunzio, L.; Girvin, S. M.; Schoelkopf, R. J. (2012). "Realization of Three-Qubit Quantum Error Correction with Superconducting Circuits". *Nature*. **482** (7385): 382–385. arXiv:1109.4948 (https://arxiv.org/abs/1109.4948). Bibcode:2012Natur.482..382R (https://ui.adsabs.harvard.edu/abs/2012Natur.482..382R). doi:10.1038/nature10786 (https://doi.org/10.1038%2Fnature10786). PMID 22297844 (https://pubmed.ncbi.nlm.nih.gov/22297844). S2CID 2610639 (https://api.semanticscholar.org/CorpusID:2610639).
26. Lassen, M.; Sabuncu, M.; Huck, A.; Niset, J.; Leuchs, G.; Cerf, N. J.; Andersen, U. L. (2010). "Quantum optical coherence can survive photon losses using a continuous-variable quantum erasure-correcting code". *Nature Photonics*. **4** (10): 700. arXiv:1006.3941 (https://arxiv.org/abs/1006.3941). Bibcode:2010NaPho...4..700L (https://ui.adsabs.harvard.edu/abs/2010NaPho...4..700L). doi:10.1038/nphoton.2010.168 (https://doi.org/10.1038%2Fnphoton.2010.168). S2CID 55090423 (https://api.semanticscholar.org/CorpusID:55090423).
27. Guo, Qihao; Zhao, Yuan-Yuan; Grassl, Markus; Nie, Xinfang; Xiang, Guo-Yong; Xin, Tao; Yin, Zhang-Qi; Zeng, Bei (2021). "Testing a quantum error-correcting code on various platforms". *Science Bulletin*. **66** (1): 29–35. arXiv:2001.07998 (https://arxiv.org/abs/2001.07998). Bibcode:2021SciBu..66...29G (https://ui.adsabs.harvard.edu/abs/2021SciBu..66...29G). doi:10.1016/j.scib.2020.07.033 (https://doi.org/10.1016%2Fj.scib.2020.07.033). PMID 36654309 (https://pubmed.ncbi.nlm.nih.gov/36654309). S2CID 210861230 (https://api.semanticscholar.org/CorpusID:210861230).
28. "Error-protected quantum bits entangled for the first time" (https://phys.org/news/2021-01-error-protected-quantum-bits-entangled.html). *phys.org*. 2021-01-13. Retrieved 2021-08-30.

29. Erhard, Alexander; Poulsen Nautrup, Hendrik; Meth, Michael; Postler, Lukas; Stricker, Roman; Stadler, Martin; Negnevitsky, Vlad; Ringbauer, Martin; Schindler, Philipp; Briegel, Hans J.; Blatt, Rainer; Friis, Nicolai; Monz, Thomas (2021-01-13). "Entangling logical qubits with lattice surgery". *Nature*. **589** (7841): 220–224. arXiv:2006.03071 (https://arxiv.org/abs/2006.03071). Bibcode:2021Natur.589..220E (https://ui.adsabs.harvard.edu/abs/2021Natur.589..220E). doi:10.1038/s41586-020-03079-6 (https://doi.org/10.1038%2Fs41586-020-03079-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 33442044 (https://pubmed.ncbi.nlm.nih.gov/33442044). S2CID 219401398 (https://api.semanticscholar.org/CorpusID:219401398).
30. Bedford, Bailey (2021-10-04). "Foundational step shows quantum computers can be better than the sum of their parts" (https://phys.org/news/2021-10-foundational-quantum-sum.html). *phys.org*. Retrieved 2021-10-05.
31. Egan, Laird; Debroy, Dripto M.; Noel, Crystal; Risinger, Andrew; Zhu, Daiwei; Biswas, Debopriyo; Newman, Michael; Li, Muyuan; Brown, Kenneth R.; Cetina, Marko; Monroe, Christopher (2021-10-04). "Fault-tolerant control of an error-corrected qubit". *Nature*. **598** (7880): 281–286. Bibcode:2021Natur.598..281E (https://ui.adsabs.harvard.edu/abs/2021Natur.598..281E). doi:10.1038/s41586-021-03928-y (https://doi.org/10.1038%2Fs41586-021-03928-y). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 34608286 (https://pubmed.ncbi.nlm.nih.gov/34608286). S2CID 238357892 (https://api.semanticscholar.org/CorpusID:238357892).
32. Ball, Philip (2021-12-23). "Real-Time Error Correction for Quantum Computing" (https://doi.org/10.1103%2FPhysics.14.184). *Physics*. **14**. 184. Bibcode:2021PhyOJ..14..184B (https://ui.adsabs.harvard.edu/abs/2021PhyOJ..14..184B). doi:10.1103/Physics.14.184 (https://doi.org/10.1103%2FPhysics.14.184). S2CID 245442996 (https://api.semanticscholar.org/CorpusID:245442996).
33. Postler, Lukas; Heußen, Sascha; Pogorelov, Ivan; Rispler, Manuel; Feldker, Thomas; Meth, Michael; Marciniak, Christian D.; Stricker, Roman; Ringbauer, Martin; Blatt, Rainer; Schindler, Philipp; Müller, Markus; Monz, Thomas (2022-05-25). "Demonstration of fault-tolerant universal quantum gate operations". *Nature*. **605** (7911): 675–680. arXiv:2111.12654 (https://arxiv.org/abs/2111.12654). Bibcode:2022Natur.605..675P (https://ui.adsabs.harvard.edu/abs/2022Natur.605..675P). doi:10.1038/s41586-022-04721-1 (https://doi.org/10.1038%2Fs41586-022-04721-1). PMID 35614250 (https://pubmed.ncbi.nlm.nih.gov/35614250). S2CID 244527180 (https://api.semanticscholar.org/CorpusID:244527180).
34. Google Quantum AI (2023-02-22). "Suppressing quantum errors by scaling a surface code logical qubit" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9946823). *Nature*. **614** (7949): 676–681. Bibcode:2023Natur.614..676G (https://ui.adsabs.harvard.edu/abs/2023Natur.614..676G). doi:10.1038/s41586-022-05434-1 (https://doi.org/10.1038%2Fs41586-022-05434-1). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9946823 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9946823). PMID 36813892 (https://pubmed.ncbi.nlm.nih.gov/36813892).
35. Boerkamp, Martijn (2023-03-20). "Breakthrough in quantum error correction could lead to large-scale quantum computers" (https://physicsworld.com/breakthrough-in-quantum-error-correction-could-lead-to-large-scale-quantum-computers/). *Physics World*. Retrieved 2023-04-01.
36. Conover, Emily (2023-02-22). "Google's quantum computer reached an error-correcting milestone" (https://www.sciencenews.org/article/google-quantum-computer-sycamore-milestone). *ScienceNews*. Retrieved 2023-04-01.
37. Smith-Goodson, Paul (2024-04-18). "Microsoft And Quantinuum Improve Quantum Error Rates By 800x" (https://www.forbes.com/sites/moorinsights/2024/04/18/microsoft-and-quantinuum-improve-quantum-error-rates-by-800x/). *Forbes*. Retrieved 2024-07-01.
38. Yirka, Bob (2024-04-05). "Quantinuum quantum computer using Microsoft's 'logical quantum bits' runs 14,000 experiments with no errors" (https://phys.org/news/2024-04-quantinuum-quantum-microsoft-logical-bits.html). *Phys.org*. Retrieved 2024-07-01.

39. Ahsan, Muhammad; Naqvi, Syed Abbas Zilqurnain; Anwer, Haider (2022-02-18). "Quantum circuit engineering for correcting coherent noise". *Physical Review A*. **105** (2): 022428. arXiv:2109.03533 (https://arxiv.org/abs/2109.03533). Bibcode:2022PhRvA.105b2428A (https://ui.adsabs.harvard.edu/abs/2022PhRvA.105b2428A). doi:10.1103/physreva.105.022428 (https://doi.org/10.1103%2Fphysreva.105.022428). ISSN 2469-9926 (https://search.worldcat.org/issn/2469-9926). S2CID 237442177 (https://api.semanticscholar.org/CorpusID:237442177).
40. Steffen, Matthias (2022-10-20). "What's the difference between error suppression, error mitigation, and error correction?" (https://research.ibm.com/blog/quantum-error-suppression-mitigation-correction). *IBM Research Blog*. Retrieved 2022-11-26.

Further reading

- Daniel Lidar and Todd Brun, ed. (2013). *Quantum Error Correction*. Cambridge University Press.
- La Guardia, Giuliano Gadioli, ed. (2020). *Quantum Error Correction: Symmetric, Asymmetric, Synchronizable, and Convolutional Codes*. Springer Nature.
- Frank Gaitan (2008). *Quantum Error Correction and Fault Tolerant Quantum Computing*. Taylor & Francis.
- Freedman, Michael H.; Meyer, David A.; Luo, Feng (2002). "Z_2-Systolic freedom and quantum codes". *Mathematics of quantum computation*. Comput. Math. Ser. Boca Raton, FL: Chapman & Hall/CRC. pp. 287–320.
- Freedman, Michael H.; Meyer, David A. (1998). "Projective plane and planar quantum codes". *Found. Comput. Math*. **2001** (3): 325–332. arXiv:quant-ph/9810055 (https://arxiv.org/abs/quant-ph/9810055). Bibcode:1998quant.ph.10055F (https://ui.adsabs.harvard.edu/abs/1998quant.ph.10055F).

External links

- "Topological Quantum Error Correction" (https://www.youtube.com/watch?v=OU9_mrxLl3g). *Quantum Light*. University of Sheffield. 2018-09-28. Archived (https://ghostarchive.org/varchive/youtube/20211222/OU9_mrxLl3g) from the original on 2021-12-22 – via YouTube.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_error_correction&oldid=1241142387"

WIKIPEDIA
The Free Encyclopedia

CSS code

In quantum error correction, **CSS codes**, named after their inventors, Robert Calderbank, Peter Shor[1] and Andrew Steane,[2] are a special type of stabilizer code constructed from classical codes with some special properties. An example of a CSS code is the Steane code.

Construction

Let C_1 and C_2 be two (classical) $[n, k_1]$, $[n, k_2]$ codes such, that $C_2 \subset C_1$ and $C_1, C_2^\perp$ both have minimal distance $\geq 2t+1$, where $C_2^\perp$ is the code dual to C_2. Then define $\mathrm{CSS}(C_1, C_2)$, the CSS code of C_1 over C_2 as an $[n, k_1 - k_2, d]$ code, with $d \geq 2t+1$ as follows:

Define for $x \in C_1 : |x + C_2\rangle := 1/\sqrt{|C_2|} \sum_{y \in C_2} |x + y\rangle$, where $+$ is bitwise addition modulo 2. Then $\mathrm{CSS}(C_1, C_2)$ is defined as $\{|x + C_2\rangle \mid x \in C_1\}$.

References

1. Robert Calderbank and Peter Shor (1996). "Good quantum error-correcting codes exist". *Physical Review A*. **54** (2): 1098–1105. arXiv:quant-ph/9512032 (https://arxiv.org/abs/quant-ph/9512032). Bibcode:1996PhRvA..54.1098C (https://ui.adsabs.harvard.edu/abs/1996PhRvA..54.1098C). doi:10.1103/PhysRevA.54.1098 (https://doi.org/10.1103%2FPhysRevA.54.1098). PMID 9913578 (https://pubmed.ncbi.nlm.nih.gov/9913578). S2CID 11524969 (https://api.semanticscholar.org/CorpusID:11524969).
2. Steane, Andrew (1996). "Multiple-Particle Interference and Quantum Error Correction". *Proc. R. Soc. Lond. A*. **452** (1954): 2551–2577. arXiv:quant-ph/9601029 (https://arxiv.org/abs/quant-ph/9601029). Bibcode:1996RSPSA.452.2551S (https://ui.adsabs.harvard.edu/abs/1996RSPSA.452.2551S). doi:10.1098/rspa.1996.0136 (https://doi.org/10.1098%2Frspa.1996.0136). S2CID 8246615 (https://api.semanticscholar.org/CorpusID:8246615).

Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum Computation and Quantum Information* (2nd ed.). Cambridge: Cambridge University Press. ISBN 978-1-107-00217-3. OCLC 844974180 (https://search.worldcat.org/oclc/844974180).

External links

Retrieved from "https://en.wikipedia.org/w/index.php?title=CSS_code&oldid=1178842410"

WIKIPEDIA
The Free Encyclopedia

Quantum convolutional code

Quantum block codes are useful in quantum computing and in quantum communications. The encoding circuit for a large block code typically has a high complexity although those for modern codes do have lower complexity.

Quantum convolutional coding theory offers a different paradigm for coding quantum information. The convolutional structure is useful for a quantum communication scenario where a sender possesses a stream of qubits to send to a receiver. The encoding circuit for a quantum convolutional code has a much lower complexity than an encoding circuit needed for a large block code. It also has a repetitive pattern so that the same physical devices or the same routines can manipulate the stream of quantum information.

Quantum convolutional stabilizer codes borrow heavily from the structure of their classical counterparts. Quantum convolutional codes are similar because some of the qubits feed back into a repeated encoding unitary and give the code a memory structure like that of a classical convolutional code. The quantum codes feature online encoding and decoding of qubits. This feature gives quantum convolutional codes both their low encoding and decoding complexity and their ability to correct a larger set of errors than a block code with similar parameters.

Definition

A quantum convolutional stabilizer code acts on a Hilbert space $\mathcal{H}$, which is a countably infinite tensor product of two-dimensional qubit Hilbert spaces indexed over integers ≥ 0 $\{\mathcal{H}_i\}_{i\in\mathbb{Z}^+}$:

$$\mathcal{H} = \bigotimes_{i=0}^{\infty} \mathcal{H}_i.$$

A sequence $\mathbf{A}$ of Pauli matrices $\{A_i\}_{i\in\mathbb{Z}^+}$, where

$$\mathbf{A} = \bigotimes_{i=0}^{\infty} A_i,$$

can act on states in $\mathcal{H}$. Let $\mathbf{\Pi}^{\mathbb{Z}^+}$ denote the set of all Pauli sequences. The support $\operatorname{supp}(\mathbf{A})$ of a Pauli sequence $\mathbf{A}$ is the set of indices of the entries in $\mathbf{A}$ that are not equal to the identity. The weight of a sequence $\mathbf{A}$ is the size $|\operatorname{supp}(\mathbf{A})|$ of its support. The delay $\operatorname{del}(\mathbf{A})$ of a sequence $\mathbf{A}$ is the smallest index for an entry not equal to the identity. The degree $\deg(\mathbf{A})$ of a sequence $\mathbf{A}$ is the largest index for an entry not equal to the identity. E.g., the following Pauli sequence

$$I \quad X \quad I \quad Y \quad Z \quad I \quad I \quad \cdots,$$

has support $\{1, 3, 4\}$, weight three, delay one, and degree four. A sequence has finite support if its weight is finite. Let $F(\mathbf{\Pi}^{\mathbb{Z}^+})$ denote the set of Pauli sequences with finite support. The following definition for a quantum convolutional code utilizes the set $F(\mathbf{\Pi}^{\mathbb{Z}^+})$ in its description.

A rate k/n-convolutional stabilizer code with $0 \leq k \leq n$ is a commuting set $\mathcal{G}$ of all n-qubit shifts of a basic generator set $\mathcal{G}_0$. The basic generator set $\mathcal{G}_0$ has $n-k$ Pauli sequences of finite support:

$$\mathcal{G}_0 = \left\{ \mathbf{G}_i \in F(\Pi^{\mathbb{Z}^+}) : 1 \leq i \leq n-k \right\}.$$

The constraint length ν of the code is the maximum degree of the generators in $\mathcal{G}_0$. A frame of the code consists of n qubits.

A quantum convolutional code admits an equivalent definition in terms of the delay transform or D-transform. The D-transform captures shifts of the basic generator set $\mathcal{G}_0$. Let us define the n-qubit delay operator D acting on any Pauli sequence $\mathbf{A} \in \Pi^{\mathbb{Z}^+}$ as follows:

$$D\left(\mathbf{A}\right) = I^{\otimes n} \otimes \mathbf{A}.$$

We can write j repeated applications of D as a power of D:

$$D^j\left(\mathbf{A}\right) = I^{\otimes jn} \otimes \mathbf{A}.$$

Let $D^j\left(\mathcal{G}_0\right)$ be the set of shifts of elements of $\mathcal{G}_0$ by j. Then the full stabilizer $\mathcal{G}$ for the convolutional stabilizer code is

$$\mathcal{G} = \bigcup_{j \in \mathbb{Z}^+} D^j\left(\mathcal{G}_0\right).$$

Operation

The operation of a convolutional stabilizer code is as follows. The protocol begins with the sender encoding a stream of qubits with an online encoding circuit such as that given in (Grassl and Roetteler 2006). The encoding circuit is *online* if it acts on a few blocks of qubits at a time. The sender transmits a set of qubits as soon as the first unitary finishes processing them. The receiver measures all the generators in $\mathcal{G}$ and corrects for errors as he receives the online encoded qubits. He finally decodes the encoded qubits with a decoding circuit. The qubits decoded from this convolutional procedure should be error free and ready for quantum computation at the receiving end.

A *finite-depth* circuit maps a Pauli sequence with finite weight to one with finite weight (Ollivier and Tillich 2004). It does not map a Pauli sequence with finite weight to one with infinite weight. This property is important because we do not want the decoding circuit to propagate uncorrected errors into the information qubit stream (Johannesson and Zigangirov 1999). A finite-depth decoding circuit corresponding to the stabilizer $\mathcal{G}$ exists by the algorithm given in (Grassl and Roetteler 2006).

Example

Forney et al. provided an example of a rate-1/3 quantum convolutional code by importing a particular classical quaternary convolutional code (Forney and Guha 2005). Grassl and Roetteler determined a noncatastrophic encoding circuit for Forney et al.'s rate-1/3 quantum convolutional code (Grassl and Roetteler 2006). The basic stabilizer and its first shift are as follows:

$$\ldots \left| \begin{matrix} I & I & I \\ I & I & I \\ I & I & I \\ I & I & I \end{matrix} \right| \left| \begin{matrix} X & X & X \\ Z & Z & Z \\ I & I & I \\ I & I & I \end{matrix} \right| \left| \begin{matrix} X & Z & Y \\ Z & Y & X \\ X & X & X \\ Z & Z & Z \end{matrix} \right| \left| \begin{matrix} I & I & I \\ I & I & I \\ X & Z & Y \\ Z & Y & X \end{matrix} \right| \left| \begin{matrix} I & I & I \\ I & I & I \\ I & I & I \\ I & I & I \end{matrix} \right| \ldots$$

The code consists of all three-qubit shifts of the above generators. The vertical bars are a visual aid to illustrate the three-qubit shifts of the basic generators. The code can correct for an arbitrary single-qubit error in every other frame.

Extensions

Wilde and Brun have integrated the theory of entanglement-assisted stabilizer codes and quantum convolutional codes in a series of articles (Wilde and Brun 2007a, 2007b, 2008, 2009) to form a theory of entanglement-assisted quantum convolutional coding. This theory supposes that a sender and receiver share noiseless bipartite entanglement that they can exploit for protecting a stream of quantum information.

(Wilde 2009), building on work of (Ollivier and Tillich 2004) and (Grassl and Roetteler 2006), also showed how to encode these codes with quantum shift register circuits, a natural extension of the theory of classical shift register circuits.

References

- Ollivier, Harold; Tillich, Jean-Pierre (2003). "Description of a Quantum Convolutional Code". *Physical Review Letters*. **91** (17): 177902. arXiv:quant-ph/0304189 (https://arxiv.org/abs/quant-ph/0304189). Bibcode:2003PhRvL..91q7902O (https://ui.adsabs.harvard.edu/abs/2003PhRvL..91q7902O). doi:10.1103/PhysRevLett.91.177902 (https://doi.org/10.1103%2FPhysRevLett.91.177902). PMID 14611378 (https://pubmed.ncbi.nlm.nih.gov/14611378). S2CID 17261900 (https://api.semanticscholar.org/CorpusID:17261900).
- Ollivier, H.; Tillich, J. -P. (2004). "Quantum convolutional codes: Fundamentals". arXiv:quant-ph/0401134 (https://arxiv.org/abs/quant-ph/0401134). Bibcode:2004quant.ph..1134O (https://ui.adsabs.harvard.edu/abs/2004quant.ph..1134O). `{{cite journal}}`: Cite journal requires `|journal=` (help)
- Forney, G. David (2005). "Simple rate-1/3 convolutional and tail-biting quantum error-correcting codes". *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005*. pp. 1028–1032. arXiv:quant-ph/0501099 (https://arxiv.org/abs/quant-ph/0501099). doi:10.1109/ISIT.2005.1523495 (https://doi.org/10.1109%2FISIT.2005.1523495). ISBN 0-7803-9151-9. S2CID 14484674 (https://api.semanticscholar.org/CorpusID:14484674).
- David Forney, G. David; Grassl, Markus; Guha, Saikat (2007). "Convolutional and Tail-Biting Quantum Error-Correcting Codes". *IEEE Transactions on Information Theory*. **53** (3): 865–880. arXiv:quant-ph/0511016 (https://arxiv.org/abs/quant-ph/0511016). doi:10.1109/TIT.2006.890698 (https://doi.org/10.1109%2FTIT.2006.890698). S2CID 546490 (https://api.semanticscholar.org/CorpusID:546490).
- M. Grassl and M. Roetteler, “Quantum convolutional codes: Encoders and structural properties,” in Forty-Fourth Annual Allerton Conference, 2006. Available at http://www.csl.illinois.edu/allerton/archives/allerton06/PDFs/papers/0285.pdf

- Grassl, Markus; Rotteler, Martin (2006). "Non-catastrophic Encoders and Encoder Inverses for Quantum Convolutional Codes". *2006 IEEE International Symposium on Information Theory*. pp. 1109–1113. arXiv:quant-ph/0602129 (https://arxiv.org/abs/quant-ph/0602129). doi:10.1109/ISIT.2006.261956 (https://doi.org/10.1109%2FISIT.2006.261956). ISBN 1-4244-0505-X. S2CID 1442 (https://api.semanticscholar.org/CorpusID:1442).
- R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Wiley-IEEE Press, 1999.
- Wilde, Mark M.; Krovi, Hari; Brun, Todd A. (2010). "Convolutional entanglement distillation". *2010 IEEE International Symposium on Information Theory*. pp. 2657–2661. arXiv:0708.3699 (https://arxiv.org/abs/0708.3699). doi:10.1109/ISIT.2010.5513666 (https://doi.org/10.1109%2FISIT.2010.5513666). ISBN 978-1-4244-7892-7. S2CID 2409176 (https://api.semanticscholar.org/CorpusID:2409176).
- Wilde, Mark M.; Brun, Todd A. (2010). "Entanglement-assisted quantum convolutional coding". *Physical Review A*. **81** (4): 042333. arXiv:0712.2223 (https://arxiv.org/abs/0712.2223). Bibcode:2010PhRvA..81d2333W (https://ui.adsabs.harvard.edu/abs/2010PhRvA..81d2333W). doi:10.1103/PhysRevA.81.042333 (https://doi.org/10.1103%2FPhysRevA.81.042333). S2CID 8410654 (https://api.semanticscholar.org/CorpusID:8410654).
- Wilde, Mark M.; Brun, Todd A. (2010). "Quantum convolutional coding with shared entanglement: General structure". *Quantum Information Processing*. **9** (5): 509–540. arXiv:0807.3803 (https://arxiv.org/abs/0807.3803). doi:10.1007/s11128-010-0179-9 (https://doi.org/10.1007%2Fs11128-010-0179-9). S2CID 18185704 (https://api.semanticscholar.org/CorpusID:18185704).
- Wilde, Mark M. (2008). "Quantum Coding with Entanglement". arXiv:0806.4214 (https://arxiv.org/abs/0806.4214). `{{cite journal}}`: Cite journal requires `|journal=` (help)
- Wilde, Mark M.; Brun, Todd A. (2009). "Extra shared entanglement reduces memory demand in quantum convolutional coding". *Physical Review A*. **79** (3): 032313. arXiv:0812.4449 (https://arxiv.org/abs/0812.4449). Bibcode:2009PhRvA..79c2313W (https://ui.adsabs.harvard.edu/abs/2009PhRvA..79c2313W). doi:10.1103/PhysRevA.79.032313 (https://doi.org/10.1103%2FPhysRevA.79.032313). S2CID 67826844 (https://api.semanticscholar.org/CorpusID:67826844).
- Wilde, Mark M. (2009). "Quantum-shift-register circuits". *Physical Review A*. **79** (6): 062325. arXiv:0903.3894 (https://arxiv.org/abs/0903.3894). Bibcode:2009PhRvA..79f2325W (https://ui.adsabs.harvard.edu/abs/2009PhRvA..79f2325W). doi:10.1103/PhysRevA.79.062325 (https://doi.org/10.1103%2FPhysRevA.79.062325). S2CID 56351003 (https://api.semanticscholar.org/CorpusID:56351003).

Further reading

Publications

- Houshmand, Monireh; Wilde, Mark M. (2013). "Recursive Quantum Convolutional Encoders are Catastrophic: A Simple Proof". *IEEE Transactions on Information Theory*. **59** (10): 6724–6731. arXiv:1209.0082 (https://arxiv.org/abs/1209.0082). doi:10.1109/TIT.2013.2272932 (https://doi.org/10.1109%2FTIT.2013.2272932). S2CID 15309497 (https://api.semanticscholar.org/CorpusID:15309497).
- Lai, Ching-Yi; Hsieh, Min-Hsiu; Lu, Hsiao-Feng (2016). "On the Mac *Williams* Identity for Classical and Quantum Convolutional Codes". *IEEE Transactions on Communications*. **64** (8): 3148–3159. arXiv:1404.5012 (https://arxiv.org/abs/1404.5012). doi:10.1109/TCOMM.2016.2585641 (https://doi.org/10.1109%2FTCOMM.2016.2585641). S2CID 7123143 (https://api.semanticscholar.org/CorpusID:7123143).

- Poulin, David; Tillich, Jean-Pierre; Ollivier, Harold (2007). "Quantum serial turbo-codes". arXiv:0712.2888 (https://arxiv.org/abs/0712.2888). {{cite journal}}: Cite journal requires |journal= (help)
- Djordjevic, Ivan (2012). *Quantum information processing and quantum error correction: an engineering approach*. Academic press. ISBN 9780123854919.
- Brun, Todd A. (2013). Lidar, Daniel A.; Brun, Todd A. (eds.). *Quantum error correction*. Cambridge University Press. arXiv:1910.03672 (https://arxiv.org/abs/1910.03672). ISBN 9780521897877.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_convolutional_code&oldid=1131657527"

WIKIPEDIA
The Free Encyclopedia

Stabilizer code

In quantum computing and quantum communication, a **stabilizer code** is a class of quantum codes for performing quantum error correction. The toric code, and surface codes more generally,[1] are types of stabilizer codes considered very important for the practical realization of quantum information processing.

Conceptual background

Quantum error-correcting codes restore a noisy, decohered quantum state to a pure quantum state. A stabilizer quantum error-correcting code appends ancilla qubits to qubits that we want to protect. A unitary encoding circuit rotates the global state into a subspace of a larger Hilbert space. This highly entangled, encoded state corrects for local noisy errors. A quantum error-correcting code makes quantum computation and quantum communication practical by providing a way for a sender and receiver to simulate a noiseless qubit channel given a noisy qubit channel whose noise conforms to a particular error model. The first quantum error-correcting codes are strikingly similar to classical block codes in their operation and performance.

The stabilizer theory of quantum error correction allows one to import some classical binary or quaternary codes for use as a quantum code. However, when importing the classical code, it must satisfy the dual-containing (or self-orthogonality) constraint. Researchers have found many examples of classical codes satisfying this constraint, but most classical codes do not. Nevertheless, it is still useful to import classical codes in this way (though, see how the entanglement-assisted stabilizer formalism overcomes this difficulty).

Mathematical background

The stabilizer formalism exploits elements of the Pauli group Π in formulating quantum error-correcting codes. The set $\Pi = \{I, X, Y, Z\}$ consists of the Pauli operators:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The above operators act on a single qubit – a state represented by a vector in a two-dimensional Hilbert space. Operators in Π have eigenvalues ± 1 and either commute or anti-commute. The set Π^n consists of n-fold tensor products of Pauli operators:

$$\Pi^n = \left\{ e^{i\phi} A_1 \otimes \cdots \otimes A_n : \forall j \in \{1, \ldots, n\} \, A_j \in \Pi, \;\; \phi \in \{0, \pi/2, \pi, 3\pi/2\} \right\}.$$

Elements of Π^n act on a quantum register of n qubits. We occasionally omit tensor product symbols in what follows so that

$$A_1 \cdots A_n \equiv A_1 \otimes \cdots \otimes A_n.$$

The n-fold Pauli group Π^n plays an important role for both the encoding circuit and the error-correction procedure of a quantum stabilizer code over n qubits.

Definition

Let us define an $[n, k]$ stabilizer quantum error-correcting code to encode k logical qubits into n physical qubits. The rate of such a code is k/n. Its stabilizer $\mathcal{S}$ is an abelian subgroup of the n-fold Pauli group Π^n. $\mathcal{S}$ does not contain the operator $-I^{\otimes n}$. The simultaneous $+1$-eigenspace of the operators constitutes the *codespace*. The codespace has dimension 2^k so that we can encode k qubits into it. The stabilizer $\mathcal{S}$ has a minimal representation in terms of $n-k$ independent generators

$$\{g_1, \ldots, g_{n-k} \mid \forall i \in \{1, \ldots, n-k\},\ g_i \in \mathcal{S}\}.$$

The generators are independent in the sense that none of them is a product of any other two (up to a global phase). The operators $g_1, \ldots, g_{n-k}$ function in the same way as a parity check matrix does for a classical linear block code.

Stabilizer error-correction conditions

One of the fundamental notions in quantum error correction theory is that it suffices to correct a discrete error set with support in the Pauli group Π^n. Suppose that the errors affecting an encoded quantum state are a subset $\mathcal{E}$ of the Pauli group Π^n:

$$\mathcal{E} \subset \Pi^n.$$

Because $\mathcal{E}$ and $\mathcal{S}$ are both subsets of Π^n, an error $E \in \mathcal{E}$ that affects an encoded quantum state either commutes or anticommutes with any particular element g in $\mathcal{S}$. The error E is correctable if it anticommutes with an element g in $\mathcal{S}$. An anticommuting error E is detectable by measuring each element g in $\mathcal{S}$ and computing a syndrome $\mathbf{r}$ identifying E. The syndrome is a binary vector $\mathbf{r}$ with length $n-k$ whose elements identify whether the error E commutes or anticommutes with each $g \in \mathcal{S}$. An error E that commutes with every element g in $\mathcal{S}$ is correctable if and only if it is in $\mathcal{S}$. It corrupts the encoded state if it commutes with every element of $\mathcal{S}$ but does not lie in $\mathcal{S}$. So we compactly summarize the stabilizer error-correcting conditions: a stabilizer code can correct any errors E_1, E_2 in $\mathcal{E}$ if

$$E_1^\dagger E_2 \notin \mathcal{Z}(\mathcal{S})$$

or

$$E_1^\dagger E_2 \in \mathcal{S}$$

where $\mathcal{Z}(\mathcal{S})$ is the centralizer of $\mathcal{S}$ (i.e., the subgroup of elements that commute with all members of $\mathcal{S}$, also known as the commutant).

Simple example of a stabilizer code

A simple example of a stabilizer code is a three qubit $[[3,1,3]]$ stabilizer code. It encodes $k=1$ logical qubit into $n=3$ physical qubits and protects against a single-bit flip error in the set $\{X_i\}$. This does not protect against other Pauli errors such as phase flip errors in the set $\{Y_i\}$.or $\{Z_i\}$. This has code distance $d=3$. Its stabilizer consists of $n-k=2$ Pauli operators:

$$\begin{array}{rcccc} g_1 & = & Z & Z & I \\ g_2 & = & I & Z & Z \end{array}$$

If there are no bit-flip errors, both operators g_1 and g_2 commute, the syndrome is +1,+1, and no errors are detected.

If there is a bit-flip error on the first encoded qubit, operator g_1 will anti-commute and g_2 commute, the syndrome is -1,+1, and the error is detected. If there is a bit-flip error on the second encoded qubit, operator g_1 will anti-commute and g_2 anti-commute, the syndrome is -1,-1, and the error is detected. If there is a bit-flip error on the third encoded qubit, operator g_1 will commute and g_2 anti-commute, the syndrome is +1,-1, and the error is detected.

Example of a stabilizer code

An example of a stabilizer code is the five qubit $[[5,1,3]]$ stabilizer code. It encodes $k=1$ logical qubit into $n=5$ physical qubits and protects against an arbitrary single-qubit error. It has code distance $d=3$. Its stabilizer consists of $n-k=4$ Pauli operators:

$$\begin{array}{rcccccc} g_1 & = & X & Z & Z & X & I \\ g_2 & = & I & X & Z & Z & X \\ g_3 & = & X & I & X & Z & Z \\ g_4 & = & Z & X & I & X & Z \end{array}$$

The above operators commute. Therefore, the codespace is the simultaneous +1-eigenspace of the above operators. Suppose a single-qubit error occurs on the encoded quantum register. A single-qubit error is in the set $\{X_i, Y_i, Z_i\}$ where A_i denotes a Pauli error on qubit i. It is straightforward to verify that any arbitrary single-qubit error has a unique syndrome. The receiver corrects any single-qubit error by identifying the syndrome via a parity measurement and applying a corrective operation.

Relation between Pauli group and binary vectors

A simple but useful mapping exists between elements of Π and the binary vector space $(\mathbb{Z}_2)^2$. This mapping gives a simplification of quantum error correction theory. It represents quantum codes with binary vectors and binary operations rather than with Pauli operators and matrix operations respectively.

We first give the mapping for the one-qubit case. Suppose $[A]$ is a set of equivalence classes of an operator A that have the same phase:

$$[A] = \{\beta A \mid \beta \in \mathbb{C},\ |\beta| = 1\}\,.$$

Let $[\Pi]$ be the set of phase-free Pauli operators where $[\Pi] = \{[A] \mid A \in \Pi\}$. Define the map $N : (\mathbb{Z}_2)^2 \to \Pi$ as

$$00 \to I,\ 01 \to X,\ 11 \to Y,\ 10 \to Z$$

Suppose $u, v \in (\mathbb{Z}_2)^2$. Let us employ the shorthand $u = (z|x)$ and $v = (z'|x')$ where z, x, z', $x' \in \mathbb{Z}_2$. For example, suppose $u = (0|1)$. Then $N(u) = X$. The map N induces an isomorphism $[N] : (\mathbb{Z}_2)^2 \to [\Pi]$ because addition of vectors in $(\mathbb{Z}_2)^2$ is equivalent to multiplication of Pauli operators up to a global phase:

$$[N(u+v)] = [N(u)]\,[N(v)]\,.$$

Let $\odot$ denote the symplectic product between two elements $u, v \in (\mathbb{Z}_2)^2$:

$$u \odot v \equiv zx' - xz'\,.$$

The symplectic product $\odot$ gives the commutation relations of elements of Π:

$$N(u)\,N(v) = (-1)^{(u \odot v)}\,N(v)\,N(u)\,.$$

The symplectic product and the mapping N thus give a useful way to phrase Pauli relations in terms of binary algebra. The extension of the above definitions and mapping N to multiple qubits is straightforward. Let $\mathbf{A} = A_1 \otimes \cdots \otimes A_n$ denote an arbitrary element of Π^n. We can similarly define the phase-free n-qubit Pauli group $[\Pi^n] = \{[\mathbf{A}] \mid \mathbf{A} \in \Pi^n\}$ where

$$[\mathbf{A}] = \{\beta\mathbf{A} \mid \beta \in \mathbb{C},\ |\beta| = 1\}\,.$$

The group operation $*$ for the above equivalence class is as follows:

$$[\mathbf{A}] * [\mathbf{B}] \equiv [A_1] * [B_1] \otimes \cdots \otimes [A_n] * [B_n] = [A_1 B_1] \otimes \cdots \otimes [A_n B_n] = [\mathbf{AB}]\,.$$

The equivalence class $[\Pi^n]$ forms a commutative group under operation $*$. Consider the $2n$-dimensional vector space

$$(\mathbb{Z}_2)^{2n} = \{(\mathbf{z}, \mathbf{x}) : \mathbf{z}, \mathbf{x} \in (\mathbb{Z}_2)^n\}\,.$$

It forms the commutative group $((\mathbb{Z}_2)^{2n}, +)$ with operation $+$ defined as binary vector addition. We employ the notation $\mathbf{u} = (\mathbf{z}|\mathbf{x})\,, \mathbf{v} = (\mathbf{z}'|\mathbf{x}')$ to represent any vectors $\mathbf{u}, \mathbf{v} \in (\mathbb{Z}_2)^{2n}$ respectively. Each vector $\mathbf{z}$ and $\mathbf{x}$ has elements $(z_1, \ldots, z_n)$ and $(x_1, \ldots, x_n)$ respectively with similar representations for $\mathbf{z}'$ and $\mathbf{x}'$. The *symplectic product* $\odot$ of $\mathbf{u}$ and $\mathbf{v}$ is

$$\mathbf{u} \odot \mathbf{v} \equiv \sum_{i=1}^{n} z_i x_i' - x_i z_i',$$

or

$$\mathbf{u} \odot \mathbf{v} \equiv \sum_{i=1}^{n} u_i \odot v_i,$$

where $u_i = (z_i|x_i)$ and $v_i = \left(z'_i|x'_i\right)$. Let us define a map $\mathbf{N} : \left(\mathbb{Z}_2\right)^{2n} \to \mathbf{\Pi}^n$ as follows:

$$\mathbf{N}\left(\mathbf{u}\right) \equiv N\left(u_1\right) \otimes \cdots \otimes N\left(u_n\right).$$

Let

$$\mathbf{X}\left(\mathbf{x}\right) \equiv X^{x_1} \otimes \cdots \otimes X^{x_n}, \quad \mathbf{Z}\left(\mathbf{z}\right) \equiv Z^{z_1} \otimes \cdots \otimes Z^{z_n},$$

so that $\mathbf{N}\left(\mathbf{u}\right)$ and $\mathbf{Z}\left(\mathbf{z}\right)\mathbf{X}\left(\mathbf{x}\right)$ belong to the same equivalence class:

$$\left[\mathbf{N}\left(\mathbf{u}\right)\right] = \left[\mathbf{Z}\left(\mathbf{z}\right)\mathbf{X}\left(\mathbf{x}\right)\right].$$

The map $\left[\mathbf{N}\right] : \left(\mathbb{Z}_2\right)^{2n} \to \left[\mathbf{\Pi}^n\right]$ is an isomorphism for the same reason given as in the previous case:

$$\left[\mathbf{N}\left(\mathbf{u}+\mathbf{v}\right)\right] = \left[\mathbf{N}\left(\mathbf{u}\right)\right]\left[\mathbf{N}\left(\mathbf{v}\right)\right],$$

where $\mathbf{u}, \mathbf{v} \in \left(\mathbb{Z}_2\right)^{2n}$. The symplectic product captures the commutation relations of any operators $\mathbf{N}\left(\mathbf{u}\right)$ and $\mathbf{N}\left(\mathbf{v}\right)$:

$$\mathbf{N}\left(\mathbf{u}\right)\mathbf{N}\left(\mathbf{v}\right) = (-1)^{\left(\mathbf{u}\odot\mathbf{v}\right)}\mathbf{N}\left(\mathbf{v}\right)\mathbf{N}\left(\mathbf{u}\right).$$

The above binary representation and symplectic algebra are useful in making the relation between classical linear error correction and quantum error correction more explicit.

By comparing quantum error correcting codes in this language to symplectic vector spaces, we can see the following. A symplectic subspace corresponds to a direct sum of Pauli algebras (i.e., encoded qubits), while an isotropic subspace corresponds to a set of stabilizers.

References

1. "What is the "surface code" in the context of quantum error correction?" (https://quantumcomputing.stackexchange.com/questions/2106/what-is-the-surface-code-in-the-context-of-quantum-error-correction). *Quantum Computing Stack Exchange*. Retrieved 2024-01-12.

- D. Gottesman, "Stabilizer codes and quantum error correction," quant-ph/9705052, Caltech Ph.D. thesis. https://arxiv.org/abs/quant-ph/9705052
- Shor, Peter W. (1995-10-01). "Scheme for reducing decoherence in quantum computer memory". *Physical Review A*. **52** (4). American Physical Society (APS): R2493–R2496. Bibcode:1995PhRvA..52.2493S (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.2493S). doi:10.1103/physreva.52.r2493 (https://doi.org/10.1103%2Fphysreva.52.r2493). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). PMID 9912632 (https://pubmed.ncbi.nlm.nih.gov/9912632).
- Calderbank, A. R.; Shor, Peter W. (1996-08-01). "Good quantum error-correcting codes exist". *Physical Review A*. **54** (2). American Physical Society (APS): 1098–1105. arXiv:quant-ph/9512032 (https://arxiv.org/abs/quant-ph/9512032). Bibcode:1996PhRvA..54.1098C (https://ui.adsabs.harvard.edu/abs/1996PhRvA..54.1098C). doi:10.1103/physreva.54.1098 (https://doi.org/10.1103%2Fphysreva.54.1098). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). PMID 9913578 (https://pubmed.ncbi.nlm.nih.gov/9913578). S2CID 11524969 (https://api.semanticscholar.org/CorpusID:11524969).

- Steane, A. M. (1996-07-29). "Error Correcting Codes in Quantum Theory". *Physical Review Letters*. **77** (5). American Physical Society (APS): 793–797. Bibcode:1996PhRvL..77..793S (https://ui.adsabs.harvard.edu/abs/1996PhRvL..77..793S). doi:10.1103/physrevlett.77.793 (https://doi.org/10.1103%2Fphysrevlett.77.793). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10062908 (https://pubmed.ncbi.nlm.nih.gov/10062908).
- A. Calderbank, E. Rains, P. Shor, and N. Sloane, “Quantum error correction via codes over GF(4),” IEEE Trans. Inf. Theory, vol. 44, pp. 1369–1387, 1998. Available at https://arxiv.org/abs/quant-ph/9608006

Retrieved from "https://en.wikipedia.org/w/index.php?title=Stabilizer_code&oldid=1197486118"

WIKIPEDIA
The Free Encyclopedia

Quantum error correction

Quantum error correction (**QEC**) is a set of techniques used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction is theorised as essential to achieve fault tolerant quantum computing that can reduce the effects of noise on stored quantum information, faulty quantum gates, faulty quantum state preparation, and faulty measurements. Effective quantum error correction would allow quantum computers with low qubit fidelity to execute algorithms of higher complexity or greater circuit depth.[1]

Classical error correction often employs redundancy. The simplest albeit inefficient approach is the repetition code. A repetition code stores the desired (logical) information as multiple copies, and—if these copies are later found to disagree due to errors introduced to the system-determines the most likely value for the original data by majority vote. E.g. suppose we copy a bit in the one (on) state three times. Suppose further that noise in the system introduces an error which corrupts the three-bit state so that one of the copied bits becomes zero (off) but the other two remain equal to one. Assuming that errors are independent and occur with some sufficiently low probability *p*, it is most likely that the error is a single-bit error and the intended message is three bits in the one state. It is possible that a double-bit error occurs and the transmitted message is equal to three zeros, but this outcome is less likely than the above outcome. In this example, the logical information is a single bit in the one state and the physical information are the three duplicate bits. Creating a physical state that represents the logical state is called *encoding* and determining which logical state is encoded in the physical state is called *decoding*. Similar to classical error correction, QEC codes do not always correctly decode logical qubits, but instead reduce the effect of noise on the logical state.

Copying quantum information is not possible due to the no-cloning theorem. This theorem seems to present an obstacle to formulating a theory of quantum error correction. But it is possible to *spread* the (logical) information of one logical qubit onto a highly entangled state of several (physical) qubits. Peter Shor first discovered this method of formulating a *quantum error correcting code* by storing the information of one qubit onto a highly entangled state of nine qubits.[2]

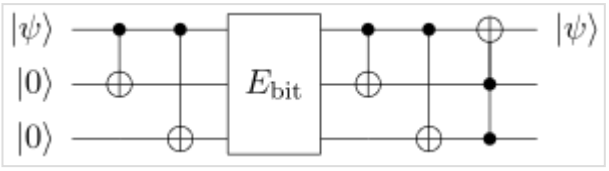
In classical error correction, *syndrome decoding* is used to diagnose which error was the likely source of corruption on an encoded state. An error can then be reversed by applying a corrective operation based on the syndrome. Quantum error correction also employs syndrome measurements. It performs a multi-qubit measurement that does not disturb the quantum information in the encoded state but retrieves information about the error. Depending on the QEC code used, syndrome measurement can determine the occurrence, location and type of errors. In most QEC codes, the type of error is either a bit flip, or a sign (of the phase) flip, or both (corresponding to the Pauli matrices X, Z, and Y). The measurement of the syndrome has the projective effect of a quantum measurement, so even if the error due to the noise was arbitrary, it can be expressed as a combination of basis operations called the error basis (which is given by the Pauli matrices and the identity). To correct the error, the Pauli operator corresponding to the type of error is used on the corrupted qubit to revert the effect of the error.

The syndrome measurement provides information about the error that has happened, but not about the information that is stored in the logical qubit—as otherwise the measurement would destroy any quantum superposition of this logical qubit with other qubits in the quantum computer, which would prevent it from being used to convey quantum information.

Bit flip code

The repetition code works in a classical channel, because classical bits are easy to measure and to repeat. This approach does not work for a quantum channel in which, due to the no-cloning theorem, it is not possible to repeat a single qubit three times. To overcome this, a different method has to be used, such as the *three-qubit bit flip code* first proposed by Asher Peres in 1985.[3] This technique uses entanglement and syndrome measurements and is comparable in performance with the repetition code.

Consider the situation in which we want to transmit the state of a single qubit $|\psi\rangle$ through a noisy channel $\mathcal{E}$. Let us moreover assume that this channel either flips the state of the qubit, with probability p, or leaves it unchanged. The action of $\mathcal{E}$ on a general input ρ can therefore be written as $\mathcal{E}(\rho) = (1-p)\rho + p\, X\rho X$.



Quantum circuit of the bit flip code

Let $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ be the quantum state to be transmitted. With no error correcting protocol in place, the transmitted state will be correctly transmitted with probability $1-p$. We can however improve on this number by *encoding* the state into a greater number of qubits, in such a way that errors in the corresponding logical qubits can be detected and corrected. In the case of the simple three-qubit repetition code, the encoding consists in the mappings $|0\rangle \to |0_{\mathrm{L}}\rangle \equiv |000\rangle$ and $|1\rangle \to |1_{\mathrm{L}}\rangle \equiv |111\rangle$. The input state $|\psi\rangle$ is encoded into the state $|\psi'\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$. This mapping can be realized for example using two CNOT gates, entangling the system with two ancillary qubits initialized in the state $|0\rangle$.[4] The encoded state $|\psi'\rangle$ is what is now passed through the noisy channel.

The channel acts on $|\psi'\rangle$ by flipping some subset (possibly empty) of its qubits. No qubit is flipped with probability $(1-p)^3$, a single qubit is flipped with probability $3p(1-p)^2$, two qubits are flipped with probability $3p^2(1-p)$, and all three qubits are flipped with probability p^3. Note that a further assumption about the channel is made here: we assume that $\mathcal{E}$ acts equally and independently on each of the three qubits in which the state is now encoded. The problem is now how to detect and correct such errors, while not corrupting the transmitted state.

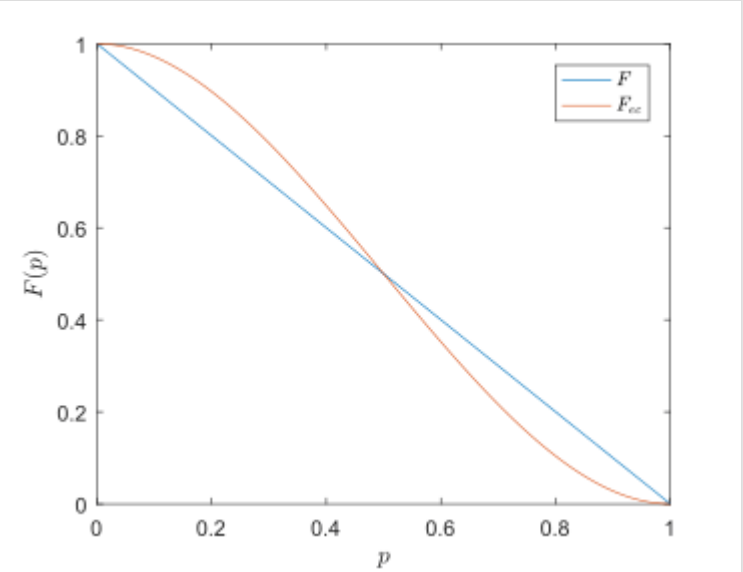
Let us assume for simplicity that p is small enough that the probability of more than a single qubit being flipped is negligible. One can then detect whether a qubit was flipped, without also querying for the values being transmitted, by asking whether one of the qubits differs from the others. This amounts to

performing a measurement with four different outcomes, corresponding to the following four projective measurements:

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|, \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned}$$

This reveals which qubits are different from the others, without at the same time giving information about the state of the qubits themselves. If the outcome corresponding to P_0 is obtained, no correction is applied, while if the outcome corresponding to P_i is observed, then the Pauli X gate is applied to the i-th qubit. Formally, this correcting procedure corresponds to the application of the following map to the output of the channel:

$$\mathcal{E}_{\text{corr}}(\rho) = P_0 \rho P_0 + \sum_{i=1}^{3} X_i P_i \rho P_i X_i.$$



Comparison of output *minimum* fidelities, with (red) and without (blue) error correcting via the three qubit bit flip code. Notice how, for $p \leq 1/2$, the error correction scheme improves the fidelity.

Note that, while this procedure perfectly corrects the output when zero or one flips are introduced by the channel, if more than one qubit is flipped then the output is not properly corrected. For example, if the first and second qubits are flipped, then the syndrome measurement gives the outcome P_3, and the third qubit is flipped, instead of the first two. To assess the performance of this error-correcting scheme for a general input we can study the fidelity $F(\psi')$ between the input $|\psi'\rangle$ and the output $\rho_{\text{out}} \equiv \mathcal{E}_{\text{corr}}(\mathcal{E}(|\psi'\rangle\langle\psi'|))$. Being the output state ρ_{out} correct when no more than one qubit is flipped, which happens with probability $(1-p)^3 + 3p(1-p)^2$, we can write it as $[(1-p)^3 + 3p(1-p)^2]\,|\psi'\rangle\langle\psi'| + (\dots)$, where the dots denote components of ρ_{out} resulting from errors not properly corrected by the protocol. It follows that

$$F(\psi') = \langle\psi'|\rho_{\text{out}}|\psi'\rangle \geq (1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3.$$

This fidelity is to be compared with the corresponding fidelity obtained when no error-correcting protocol is used, which was shown before to equal $1-p$. A little algebra then shows that the fidelity *after* error correction is greater than the one without for $p < 1/2$. Note that this is consistent with the working assumption that was made while deriving the protocol (of p being small enough).

Sign flip code

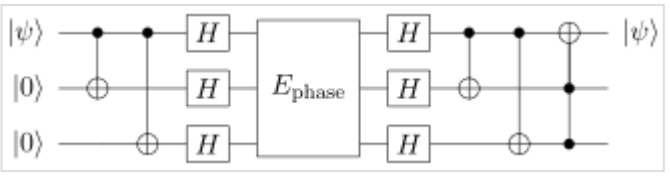
Flipped bits are the only kind of error in classical computer, but there is another possibility of an error with quantum computers, the sign flip. Through the transmission in a channel the relative sign between $|0\rangle$ and $|1\rangle$ can become inverted. For instance, a qubit in the state $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ may have its sign flip to $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

The original state of the qubit

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$

will be changed into the state

$$|\psi'\rangle = \alpha_0|{+}{+}{+}\rangle + \alpha_1|{-}{-}{-}\rangle.$$



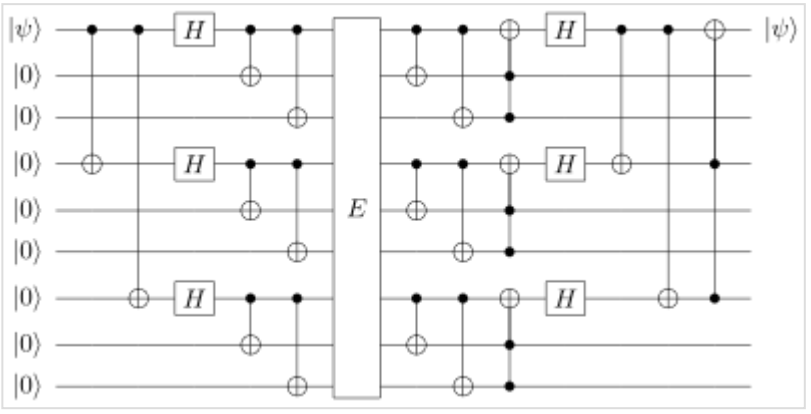
Quantum circuit of the phase flip code

In the Hadamard basis, bit flips become sign flips and sign flips become bit flips. Let $\boldsymbol{E_{\text{phase}}}$ be a quantum channel that can cause at most one phase flip. Then the bit flip code from above can recover $|\psi\rangle$ by transforming into the Hadamard basis before and after transmission through $\boldsymbol{E_{\text{phase}}}$.

Shor code

The error channel may induce either a bit flip, a sign flip (i.e., a phase flip), or both. It is possible to correct for both types of errors on a logical qubit using a well-designed QEC code. One example of a code that does this is the Shor code, published in 1995.[2][5]:10 Since these two types of errors are the only types of errors that can result after a projective measurement, a Shor code corrects arbitrary single-qubit errors.

Let $\boldsymbol{E}$ be a quantum channel that can arbitrarily corrupt a single qubit. The 1st, 4th and 7th qubits are for the sign flip code, while the three groups of qubits (1,2,3), (4,5,6), and (7,8,9) are designed for the bit flip code. With the Shor code, a qubit state $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ will be transformed into the product of 9 qubits $|\psi'\rangle = \alpha_0|0_S\rangle + \alpha_1|1_S\rangle$, where



Quantum circuit to encode a single logical qubit with the Shor code and then perform bit flip error correction on each of the three blocks.

$$|0_S\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1_S\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

If a bit flip error happens to a qubit, the syndrome analysis will be performed on each block of qubits (1,2,3), (4,5,6), and (7,8,9) to detect and correct at most one bit flip error in each block.

If the three bit flip group (1,2,3), (4,5,6), and (7,8,9) are considered as three inputs, then the Shor code circuit can be reduced as a sign flip code. This means that the Shor code can also repair a sign flip error for a single qubit.

The Shor code also can correct for any arbitrary errors (both bit flip and sign flip) to a single qubit. If an error is modeled by a unitary transform U, which will act on a qubit $|\psi\rangle$, then U can be described in the form

$$U = c_0 I + c_1 X + c_2 Y + c_3 Z$$

where c_0,c_1,c_2, and c_3 are complex constants, I is the identity, and the Pauli matrices are given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix};$$
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

If *U* is equal to *I*, then no error occurs. If $U = X$, a bit flip error occurs. If $U = Z$, a sign flip error occurs. If $U = iY$ then both a bit flip error and a sign flip error occur. In other words, the Shor code can correct any combination of bit or phase errors on a single qubit.

Bosonic codes

Several proposals have been made for storing error-correctable quantum information in bosonic modes. Unlike a two-level system, a quantum harmonic oscillator has infinitely many energy levels in a single physical system. Codes for these systems include cat,[6][7][8] Gottesman-Kitaev-Preskill (GKP),[9] and binomial codes.[10][11] One insight offered by these codes is to take advantage of the redundancy within a single system, rather than to duplicate many two-level qubits.

Binomial code[10]

Written in the Fock basis, the simplest binomial encoding is

$$|0_\mathrm{L}\rangle = \frac{|0\rangle + |4\rangle}{\sqrt{2}}, \quad |1_\mathrm{L}\rangle = |2\rangle,$$

where the subscript L indicates a "logically encoded" state. Then if the dominant error mechanism of the system is the stochastic application of the bosonic lowering operator $\hat{a}$, the corresponding error states are $|3\rangle$ and $|1\rangle$, respectively. Since the codewords involve only even photon number, and the error states involve only odd photon number, errors can be detected by measuring the photon number parity of the system.[10][12] Measuring the odd parity will allow correction by application of an appropriate unitary operation without knowledge of the specific logical state of the qubit. However, the particular binomial code above is not robust to two-photon loss.

Cat code[6][7][8]

Schrödinger cat states, superpositions of coherent states, can also be used as logical states for error correction codes. Cat code, realized by Ofek et al.[13] in 2016, defined two sets of logical states: $\{|0_L^+\rangle, |1_L^+\rangle\}$ and $\{|0_L^-\rangle, |1_L^-\rangle\}$, where each of the states is a superposition of coherent state as follows

$$
\begin{aligned}
|0_L^+\rangle &\equiv |\alpha\rangle + |-\alpha\rangle, \\
|1_L^+\rangle &\equiv |i\alpha\rangle + |-i\alpha\rangle, \\
|0_L^-\rangle &\equiv |\alpha\rangle - |-\alpha\rangle, \\
|1_L^-\rangle &\equiv |i\alpha\rangle - |-i\alpha\rangle.
\end{aligned}
$$

Those two sets of states differ from the photon number parity, as states denoted with $^+$ only occupy even photon number states and states with $^-$ indicate they have odd parity. Similar to the binomial code, if the dominant error mechanism of the system is the stochastic application of the bosonic lowering operator $\hat{a}$, the error takes the logical states from the even parity subspace to the odd one, and vice versa. Single-photon-loss errors can therefore be detected by measuring the photon number parity operator $\exp(i\pi\hat{a}^\dagger\hat{a})$ using a dispersively coupled ancillary qubit.[12]

Still, cat qubits are not protected against two-photon loss $\hat{a}^2$, dephasing noise $\hat{a}^\dagger\hat{a}$, photon-gain error $\hat{a}^\dagger$, etc.

General codes

In general, a *quantum code* for a quantum channel $\mathcal{E}$ is a subspace $\mathcal{C} \subseteq \mathcal{H}$, where $\mathcal{H}$ is the state Hilbert space, such that there exists another quantum channel $\mathcal{R}$ with

$$(\mathcal{R} \circ \mathcal{E})(\rho) = \rho \quad \forall \rho = P_{\mathcal{C}} \rho P_{\mathcal{C}},$$

where $P_{\mathcal{C}}$ is the orthogonal projection onto $\mathcal{C}$. Here $\mathcal{R}$ is known as the *correction operation*.

A *non-degenerate code* is one for which different elements of the set of correctable errors produce linearly independent results when applied to elements of the code. If distinct of the set of correctable errors produce orthogonal results, the code is considered *pure*.[14]

Models

Over time, researchers have come up with several codes:

- Peter Shor's 9-qubit-code, a.k.a. the Shor code, encodes 1 logical qubit in 9 physical qubits and can correct for arbitrary errors in a single qubit.
- Andrew Steane found a code that does the same with 7 instead of 9 qubits, see Steane code.
- Raymond Laflamme and collaborators found a class of 5-qubit codes that do the same, which also have the property of being fault-tolerant. A 5-qubit code is the smallest possible code that protects a single logical qubit against single-qubit errors.
- A generalisation of the technique used by Steane, to develop the 7-qubit code from the classical [7, 4] Hamming code, led to the construction of an important class of codes called the CSS codes, named for their inventors: Robert Calderbank, Peter Shor and Andrew Steane. According to the quantum Hamming bound, encoding a single logical qubit and providing for arbitrary error correction in a single qubit requires a minimum of 5 physical qubits.
- A more general class of codes (encompassing the former) are the stabilizer codes discovered by Daniel Gottesman, and by Robert Calderbank, Eric Rains, Peter Shor, and N. J. A. Sloane; these are also called additive codes.

- Two dimensional Bacon–Shor codes are a family of codes parameterized by integers *m* and *n*. There are *nm* qubits arranged in a square lattice.[15]
- Alexei Kitaev's topological quantum codes, introduced in 1997 as the toric code, and the more general idea of a topological quantum computer are the basis for various code types.[16]
- Todd Brun, Igor Devetak, and Min-Hsiu Hsieh also constructed the entanglement-assisted stabilizer formalism as an extension of the standard stabilizer formalism that incorporates quantum entanglement shared between a sender and a receiver.
- The ideas of stabilizer codes, CSS codes, and topological codes can be expanded into the 2D planar surface code, of which various types exist.[17] As of June 2024, the 2D planar surface code is generally considered the most well-studied type of quantum error correction, and one of the leading contenders for practical use in quantum computing. [18][19]

That these codes allow indeed for quantum computations of arbitrary length is the content of the quantum threshold theorem, found by Michael Ben-Or and Dorit Aharonov, which asserts that you can correct for all errors if you concatenate quantum codes such as the CSS codes—i.e. re-encode each logical qubit by the same code again, and so on, on logarithmically many levels—*provided* that the error rate of individual quantum gates is below a certain threshold; as otherwise, the attempts to measure the syndrome and correct the errors would introduce more new errors than they correct for.

As of late 2004, estimates for this threshold indicate that it could be as high as 1–3%,[20] provided that there are sufficiently many qubits available.

Experimental realization

There have been several experimental realizations of CSS-based codes. The first demonstration was with nuclear magnetic resonance qubits.[21] Subsequently, demonstrations have been made with linear optics,[22] trapped ions,[23][24] and superconducting (transmon) qubits.[25]

In 2016 for the first time the lifetime of a quantum bit was prolonged by employing a QEC code.[13] The error-correction demonstration was performed on Schrodinger-cat states encoded in a superconducting resonator, and employed a quantum controller capable of performing real-time feedback operations including read-out of the quantum information, its analysis, and the correction of its detected errors. The work demonstrated how the quantum-error-corrected system reaches the break-even point at which the lifetime of a logical qubit exceeds the lifetime of the underlying constituents of the system (the physical qubits).

Other error correcting codes have also been implemented, such as one aimed at correcting for photon loss, the dominant error source in photonic qubit schemes.[26][27]

In 2021, an entangling gate between two logical qubits encoded in topological quantum error-correction codes has first been realized using 10 ions in a trapped-ion quantum computer.[28][29] 2021 also saw the first experimental demonstration of fault-tolerant Bacon-Shor code in a single logical qubit of a trapped-ion system, i.e. a demonstration for which the addition of error correction is able to suppress more errors than is introduced by the overhead required to implement the error correction as well as fault tolerant Steane code.[30][31][32]

In 2022, researchers at the University of Innsbruck have demonstrated a fault-tolerant universal set of gates on two logical qubits in a trapped-ion quantum computer. They have performed a logical two-qubit controlled-NOT gate between two instances of the seven-qubit colour code, and fault-tolerantly prepared a logical magic state.[33]

In February 2023 researchers at Google claimed to have decreased quantum errors by increasing the qubit number in experiments, they used a fault tolerant surface code measuring an error rate of 3.028% and 2.914% for a distance-3 qubit array and a distance-5 qubit array respectively.[34][35][36]

In April 2024, researchers at Microsoft claimed to have successfully tested a quantum error correction code that allowed them to achieve an error rate with logical qubits that is 800 times better than the underlying physical error rate.[37]

This qubit virtualization system was used to create 4 logical qubits with 30 of the 32 qubits on Quantinuum's trapped-ion hardware. The system uses an active syndrome extraction technique to diagnose errors and correct them while calculations are underway without destroying the logical qubits.[38]

Quantum error-correction without encoding and parity-checks

In 2022, research at University of Engineering and Technology Lahore demonstrated error-cancellation by inserting single-qubit Z-axis rotation gates into strategically chosen locations of the superconductor quantum circuits.[39] The scheme has been shown to effectively correct errors that would otherwise rapidly add up under constructive interference of coherent noise. This is a circuit-level calibration scheme that traces deviations (e.g. sharp dips or notches) in the decoherence curve to detect and localize the coherent error, but does not require encoding or parity measurements.[40] However, further investigation is needed to establish the effectiveness of this method for the incoherent noise.[39]

See also

- Error detection and correction
- Soft error

References

1. Cai, Weizhou; Ma, Yuwei (2021). "Bosonic quantum error correction codes in superconducting quantum circuits" (https://doi.org/10.1016%2Fj.fmre.2020.12.006). *Fundamental Research*. **1** (1): 50–67. arXiv:2010.08699 (https://arxiv.org/abs/2010.08699). Bibcode:2021FunRe...1...50C (https://ui.adsabs.harvard.edu/abs/2021FunRe...1...50C). doi:10.1016/j.fmre.2020.12.006 (https://doi.org/10.1016%2Fj.fmre.2020.12.006). "A practical quantum computer that is capable of large circuit depth, therefore, ultimately calls for operations on logical qubits protected by quantum error correction"

2. Shor, Peter W. (1995). "Scheme for reducing decoherence in quantum computer memory". *Physical Review A*. **52** (4): R2493–R2496. Bibcode:1995PhRvA..52.2493S (https://ui.adsabs.harvard.edu/abs/1995PhRvA..52.2493S). doi:10.1103/PhysRevA.52.R2493 (https://doi.org/10.1103%2FPhysRevA.52.R2493). PMID 9912632 (https://pubmed.ncbi.nlm.nih.gov/9912632).
3. Peres, Asher (1985). "Reversible Logic and Quantum Computers". *Physical Review A*. **32** (6): 3266–3276. Bibcode:1985PhRvA..32.3266P (https://ui.adsabs.harvard.edu/abs/1985PhRvA..32.3266P). doi:10.1103/PhysRevA.32.3266 (https://doi.org/10.1103%2FPhysRevA.32.3266). PMID 9896493 (https://pubmed.ncbi.nlm.nih.gov/9896493).
4. Nielsen, Michael A.; Chuang, Isaac L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.
5. Devitt, Simon J; Munro, William J; Nemoto, Kae (2013-06-20). "Quantum error correction for beginners" (https://dx.doi.org/10.1088/0034-4885/76/7/076001). *Reports on Progress in Physics*. **76** (7): 076001. arXiv:0905.2794 (https://arxiv.org/abs/0905.2794). Bibcode:2013RPPh...76g6001D (https://ui.adsabs.harvard.edu/abs/2013RPPh...76g6001D). doi:10.1088/0034-4885/76/7/076001 (https://doi.org/10.1088%2F0034-4885%2F76%2F7%2F076001). ISSN 0034-4885 (https://search.worldcat.org/issn/0034-4885). PMID 23787909 (https://pubmed.ncbi.nlm.nih.gov/23787909). S2CID 206021660 (https://api.semanticscholar.org/CorpusID:206021660).
6. Cochrane, P. T.; Milburn, G. J.; Munro, W. J. (1999-04-01). "Macroscopically distinct quantum-superposition states as a bosonic code for amplitude damping". *Physical Review A*. **59** (4): 2631–2634. arXiv:quant-ph/9809037 (https://arxiv.org/abs/quant-ph/9809037). Bibcode:1999PhRvA..59.2631C (https://ui.adsabs.harvard.edu/abs/1999PhRvA..59.2631C). doi:10.1103/PhysRevA.59.2631 (https://doi.org/10.1103%2FPhysRevA.59.2631). S2CID 119532538 (https://api.semanticscholar.org/CorpusID:119532538).
7. Leghtas, Zaki; Kirchmair, Gerhard; Vlastakis, Brian; Schoelkopf, Robert J.; Devoret, Michel H.; Mirrahimi, Mazyar (2013-09-20). "Hardware-Efficient Autonomous Quantum Memory Protection". *Physical Review Letters*. **111** (12): 120501. arXiv:1207.0679 (https://arxiv.org/abs/1207.0679). Bibcode:2013PhRvL.111l0501L (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111l0501L). doi:10.1103/physrevlett.111.120501 (https://doi.org/10.1103%2Fphysrevlett.111.120501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 24093235 (https://pubmed.ncbi.nlm.nih.gov/24093235). S2CID 19929020 (https://api.semanticscholar.org/CorpusID:19929020).
8. Mirrahimi, Mazyar; Leghtas, Zaki; Albert, Victor V; Touzard, Steven; Schoelkopf, Robert J; Jiang, Liang; Devoret, Michel H (2014-04-22). "Dynamically protected cat-qubits: a new paradigm for universal quantum computation". *New Journal of Physics*. **16** (4): 045014. arXiv:1312.2017 (https://arxiv.org/abs/1312.2017). Bibcode:2014NJPh...16d5014M (https://ui.adsabs.harvard.edu/abs/2014NJPh...16d5014M). doi:10.1088/1367-2630/16/4/045014 (https://doi.org/10.1088%2F1367-2630%2F16%2F4%2F045014). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 7179816 (https://api.semanticscholar.org/CorpusID:7179816).
9. Daniel Gottesman; Alexei Kitaev; John Preskill (2001). "Encoding a qubit in an oscillator". *Physical Review A*. **64** (1): 012310. arXiv:quant-ph/0008040 (https://arxiv.org/abs/quant-ph/0008040). Bibcode:2001PhRvA..64a2310G (https://ui.adsabs.harvard.edu/abs/2001PhRvA..64a2310G). doi:10.1103/PhysRevA.64.012310 (https://doi.org/10.1103%2FPhysRevA.64.012310). S2CID 18995200 (https://api.semanticscholar.org/CorpusID:18995200).
10. Michael, Marios H.; Silveri, Matti; Brierley, R. T.; Albert, Victor V.; Salmilehto, Juha; Jiang, Liang; Girvin, S. M. (2016-07-14). "New Class of Quantum Error-Correcting Codes for a Bosonic Mode". *Physical Review X*. **6** (3): 031006. arXiv:1602.00008 (https://arxiv.org/abs/1602.00008). Bibcode:2016PhRvX...6c1006M (https://ui.adsabs.harvard.edu/abs/2016PhRvX...6c1006M). doi:10.1103/PhysRevX.6.031006 (https://doi.org/10.1103%2FPhysRevX.6.031006). S2CID 29518512 (https://api.semanticscholar.org/CorpusID:29518512).

11. Albert, Victor V.; Noh, Kyungjoo; Duivenvoorden, Kasper; Young, Dylan J.; Brierley, R. T.; Reinhold, Philip; Vuillot, Christophe; Li, Linshu; Shen, Chao; Girvin, S. M.; Terhal, Barbara M.; Jiang, Liang (2018). "Performance and structure of single-mode bosonic codes". *Physical Review A*. **97** (3): 032346. arXiv:1708.05010 (https://arxiv.org/abs/1708.05010). Bibcode:2018PhRvA..97c2346A (https://ui.adsabs.harvard.edu/abs/2018PhRvA..97c2346A). doi:10.1103/PhysRevA.97.032346 (https://doi.org/10.1103%2FPhysRevA.97.032346). S2CID 51691343 (https://api.semanticscholar.org/CorpusID:51691343).
12. Sun, L.; Petrenko, A.; Leghtas, Z.; Vlastakis, B.; Kirchmair, G.; Sliwa, K. M.; Narla, A.; Hatridge, M.; Shankar, S.; Blumoff, J.; Frunzio, L.; Mirrahimi, M.; Devoret, M. H.; Schoelkopf, R. J. (July 2014). "Tracking photon jumps with repeated quantum non-demolition parity measurements". *Nature*. **511** (7510): 444–448. arXiv:1311.2534 (https://arxiv.org/abs/1311.2534). Bibcode:2014Natur.511..444S (https://ui.adsabs.harvard.edu/abs/2014Natur.511..444S). doi:10.1038/nature13436 (https://doi.org/10.1038%2Fnature13436). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 25043007 (https://pubmed.ncbi.nlm.nih.gov/25043007). S2CID 987945 (https://api.semanticscholar.org/CorpusID:987945).
13. Ofek, Nissim; Petrenko, Andrei; Heeres, Reinier; Reinhold, Philip; Leghtas, Zaki; Vlastakis, Brian; Liu, Yehan; Frunzio, Luigi; Girvin, S. M.; Jiang, L.; Mirrahimi, Mazyar (August 2016). "Extending the lifetime of a quantum bit with error correction in superconducting circuits". *Nature*. **536** (7617): 441–445. Bibcode:2016Natur.536..441O (https://ui.adsabs.harvard.edu/abs/2016Natur.536..441O). doi:10.1038/nature18949 (https://doi.org/10.1038%2Fnature18949). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 27437573 (https://pubmed.ncbi.nlm.nih.gov/27437573). S2CID 594116 (https://api.semanticscholar.org/CorpusID:594116).
14. Calderbank, A. R.; Rains, E. M.; Shor, P. W.; Sloane, N. J. A. (1998). "Quantum Error Correction via Codes over GF(4)". *IEEE Transactions on Information Theory*. **44** (4): 1369–1387. arXiv:quant-ph/9608006 (https://arxiv.org/abs/quant-ph/9608006). doi:10.1109/18.681315 (https://doi.org/10.1109%2F18.681315). S2CID 1215697 (https://api.semanticscholar.org/CorpusID:1215697).
15. Bacon, Dave (2006-01-30). "Operator quantum error-correcting subsystems for self-correcting quantum memories". *Physical Review A*. **73** (1): 012340. arXiv:quant-ph/0506023 (https://arxiv.org/abs/quant-ph/0506023). Bibcode:2006PhRvA..73a2340B (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73a2340B). doi:10.1103/PhysRevA.73.012340 (https://doi.org/10.1103%2FPhysRevA.73.012340). S2CID 118968017 (https://api.semanticscholar.org/CorpusID:118968017).
16. Kitaev, Alexei (1997-07-31). "Quantum Error Correction with Imperfect Gates" (https://link.springer.com/book/10.1007/978-1-4615-5923-8). *Quantum Communication, Computing, and Measurement*. Springer. pp. 181–188. doi:10.1007/978-1-4615-5923-8 (https://doi.org/10.1007%2F978-1-4615-5923-8).
17. Fowler, Austin G.; Mariantoni, Matteo; Martinis, John M.; Cleland, Andrew N. (2012-09-18). "Surface codes: Towards practical large-scale quantum computation". *Physical Review A*. **86** (3): 032324. arXiv:1208.0928 (https://arxiv.org/abs/1208.0928). Bibcode:2012PhRvA..86c2324F (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86c2324F). doi:10.1103/PhysRevA.86.032324 (https://doi.org/10.1103%2FPhysRevA.86.032324). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947).
18. Gidney, Craig; Newman, Michael; Brooks, Peter; Jones, Cody (2023). "Yoked surface codes". arXiv:2312.04522 (https://arxiv.org/abs/2312.04522) [quant-ph (https://arxiv.org/archive/quant-ph)].
19. Horsman, Dominic; Fowler, Austin G; Devitt, Simon; Meter, Rodney Van (2012-12-01). "Surface code quantum computing by lattice surgery". *New Journal of Physics*. **14** (12): 123011. arXiv:1111.4022 (https://arxiv.org/abs/1111.4022). Bibcode:2012NJPh...14l3011H (https://ui.adsabs.harvard.edu/abs/2012NJPh...14l3011H). doi:10.1088/1367-2630/14/12/123011 (https://doi.org/10.1088%2F1367-2630%2F14%2F12%2F123011). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).

20. Knill, Emanuel (2004-11-02). "Quantum Computing with Very Noisy Devices". *Nature*. **434** (7029): 39–44. arXiv:quant-ph/0410199 (https://arxiv.org/abs/quant-ph/0410199). Bibcode:2005Natur.434...39K (https://ui.adsabs.harvard.edu/abs/2005Natur.434...39K). doi:10.1038/nature03350 (https://doi.org/10.1038%2Fnature03350). PMID 15744292 (https://pubmed.ncbi.nlm.nih.gov/15744292). S2CID 4420858 (https://api.semanticscholar.org/CorpusID:4420858).
21. Cory, D. G.; Price, M. D.; Maas, W.; Knill, E.; Laflamme, R.; Zurek, W. H.; Havel, T. F.; Somaroo, S. S. (1998). "Experimental Quantum Error Correction". *Phys. Rev. Lett*. **81** (10): 2152–2155. arXiv:quant-ph/9802018 (https://arxiv.org/abs/quant-ph/9802018). Bibcode:1998PhRvL..81.2152C (https://ui.adsabs.harvard.edu/abs/1998PhRvL..81.2152C). doi:10.1103/PhysRevLett.81.2152 (https://doi.org/10.1103%2FPhysRevLett.81.2152). S2CID 11662810 (https://api.semanticscholar.org/CorpusID:11662810).
22. Pittman, T. B.; Jacobs, B. C.; Franson, J. D. (2005). "Demonstration of quantum error correction using linear optics". *Phys. Rev. A*. **71** (5): 052332. arXiv:quant-ph/0502042 (https://arxiv.org/abs/quant-ph/0502042). Bibcode:2005PhRvA..71e2332P (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71e2332P). doi:10.1103/PhysRevA.71.052332 (https://doi.org/10.1103%2FPhysRevA.71.052332). S2CID 11679660 (https://api.semanticscholar.org/CorpusID:11679660).
23. Chiaverini, J.; Leibfried, D.; Schaetz, T.; Barrett, M. D.; Blakestad, R. B.; Britton, J.; Itano, W. M.; Jost, J. D.; Knill, E.; Langer, C.; Ozeri, R.; Wineland, D. J. (2004). "Realization of quantum error correction". *Nature*. **432** (7017): 602–605. Bibcode:2004Natur.432..602C (https://ui.adsabs.harvard.edu/abs/2004Natur.432..602C). doi:10.1038/nature03074 (https://doi.org/10.1038%2Fnature03074). PMID 15577904 (https://pubmed.ncbi.nlm.nih.gov/15577904). S2CID 167898 (https://api.semanticscholar.org/CorpusID:167898).
24. Schindler, P.; Barreiro, J. T.; Monz, T.; Nebendahl, V.; Nigg, D.; Chwalla, M.; Hennrich, M.; Blatt, R. (2011). "Experimental Repetitive Quantum Error Correction". *Science*. **332** (6033): 1059–1061. Bibcode:2011Sci...332.1059S (https://ui.adsabs.harvard.edu/abs/2011Sci...332.1059S). doi:10.1126/science.1203329 (https://doi.org/10.1126%2Fscience.1203329). PMID 21617070 (https://pubmed.ncbi.nlm.nih.gov/21617070). S2CID 32268350 (https://api.semanticscholar.org/CorpusID:32268350).
25. Reed, M. D.; DiCarlo, L.; Nigg, S. E.; Sun, L.; Frunzio, L.; Girvin, S. M.; Schoelkopf, R. J. (2012). "Realization of Three-Qubit Quantum Error Correction with Superconducting Circuits". *Nature*. **482** (7385): 382–385. arXiv:1109.4948 (https://arxiv.org/abs/1109.4948). Bibcode:2012Natur.482..382R (https://ui.adsabs.harvard.edu/abs/2012Natur.482..382R). doi:10.1038/nature10786 (https://doi.org/10.1038%2Fnature10786). PMID 22297844 (https://pubmed.ncbi.nlm.nih.gov/22297844). S2CID 2610639 (https://api.semanticscholar.org/CorpusID:2610639).
26. Lassen, M.; Sabuncu, M.; Huck, A.; Niset, J.; Leuchs, G.; Cerf, N. J.; Andersen, U. L. (2010). "Quantum optical coherence can survive photon losses using a continuous-variable quantum erasure-correcting code". *Nature Photonics*. **4** (10): 700. arXiv:1006.3941 (https://arxiv.org/abs/1006.3941). Bibcode:2010NaPho...4..700L (https://ui.adsabs.harvard.edu/abs/2010NaPho...4..700L). doi:10.1038/nphoton.2010.168 (https://doi.org/10.1038%2Fnphoton.2010.168). S2CID 55090423 (https://api.semanticscholar.org/CorpusID:55090423).
27. Guo, Qihao; Zhao, Yuan-Yuan; Grassl, Markus; Nie, Xinfang; Xiang, Guo-Yong; Xin, Tao; Yin, Zhang-Qi; Zeng, Bei (2021). "Testing a quantum error-correcting code on various platforms". *Science Bulletin*. **66** (1): 29–35. arXiv:2001.07998 (https://arxiv.org/abs/2001.07998). Bibcode:2021SciBu..66...29G (https://ui.adsabs.harvard.edu/abs/2021SciBu..66...29G). doi:10.1016/j.scib.2020.07.033 (https://doi.org/10.1016%2Fj.scib.2020.07.033). PMID 36654309 (https://pubmed.ncbi.nlm.nih.gov/36654309). S2CID 210861230 (https://api.semanticscholar.org/CorpusID:210861230).
28. "Error-protected quantum bits entangled for the first time" (https://phys.org/news/2021-01-error-protected-quantum-bits-entangled.html). *phys.org*. 2021-01-13. Retrieved 2021-08-30.

29. Erhard, Alexander; Poulsen Nautrup, Hendrik; Meth, Michael; Postler, Lukas; Stricker, Roman; Stadler, Martin; Negnevitsky, Vlad; Ringbauer, Martin; Schindler, Philipp; Briegel, Hans J.; Blatt, Rainer; Friis, Nicolai; Monz, Thomas (2021-01-13). "Entangling logical qubits with lattice surgery". *Nature*. **589** (7841): 220–224. arXiv:2006.03071 (https://arxiv.org/abs/2006.03071). Bibcode:2021Natur.589..220E (https://ui.adsabs.harvard.edu/abs/2021Natur.589..220E). doi:10.1038/s41586-020-03079-6 (https://doi.org/10.1038%2Fs41586-020-03079-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 33442044 (https://pubmed.ncbi.nlm.nih.gov/33442044). S2CID 219401398 (https://api.semanticscholar.org/CorpusID:219401398).
30. Bedford, Bailey (2021-10-04). "Foundational step shows quantum computers can be better than the sum of their parts" (https://phys.org/news/2021-10-foundational-quantum-sum.html). *phys.org*. Retrieved 2021-10-05.
31. Egan, Laird; Debroy, Dripto M.; Noel, Crystal; Risinger, Andrew; Zhu, Daiwei; Biswas, Debopriyo; Newman, Michael; Li, Muyuan; Brown, Kenneth R.; Cetina, Marko; Monroe, Christopher (2021-10-04). "Fault-tolerant control of an error-corrected qubit". *Nature*. **598** (7880): 281–286. Bibcode:2021Natur.598..281E (https://ui.adsabs.harvard.edu/abs/2021Natur.598..281E). doi:10.1038/s41586-021-03928-y (https://doi.org/10.1038%2Fs41586-021-03928-y). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 34608286 (https://pubmed.ncbi.nlm.nih.gov/34608286). S2CID 238357892 (https://api.semanticscholar.org/CorpusID:238357892).
32. Ball, Philip (2021-12-23). "Real-Time Error Correction for Quantum Computing" (https://doi.org/10.1103%2FPhysics.14.184). *Physics*. **14**. 184. Bibcode:2021PhyOJ..14..184B (https://ui.adsabs.harvard.edu/abs/2021PhyOJ..14..184B). doi:10.1103/Physics.14.184 (https://doi.org/10.1103%2FPhysics.14.184). S2CID 245442996 (https://api.semanticscholar.org/CorpusID:245442996).
33. Postler, Lukas; Heußen, Sascha; Pogorelov, Ivan; Rispler, Manuel; Feldker, Thomas; Meth, Michael; Marciniak, Christian D.; Stricker, Roman; Ringbauer, Martin; Blatt, Rainer; Schindler, Philipp; Müller, Markus; Monz, Thomas (2022-05-25). "Demonstration of fault-tolerant universal quantum gate operations". *Nature*. **605** (7911): 675–680. arXiv:2111.12654 (https://arxiv.org/abs/2111.12654). Bibcode:2022Natur.605..675P (https://ui.adsabs.harvard.edu/abs/2022Natur.605..675P). doi:10.1038/s41586-022-04721-1 (https://doi.org/10.1038%2Fs41586-022-04721-1). PMID 35614250 (https://pubmed.ncbi.nlm.nih.gov/35614250). S2CID 244527180 (https://api.semanticscholar.org/CorpusID:244527180).
34. Google Quantum AI (2023-02-22). "Suppressing quantum errors by scaling a surface code logical qubit" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9946823). *Nature*. **614** (7949): 676–681. Bibcode:2023Natur.614..676G (https://ui.adsabs.harvard.edu/abs/2023Natur.614..676G). doi:10.1038/s41586-022-05434-1 (https://doi.org/10.1038%2Fs41586-022-05434-1). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 9946823 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9946823). PMID 36813892 (https://pubmed.ncbi.nlm.nih.gov/36813892).
35. Boerkamp, Martijn (2023-03-20). "Breakthrough in quantum error correction could lead to large-scale quantum computers" (https://physicsworld.com/breakthrough-in-quantum-error-correction-could-lead-to-large-scale-quantum-computers/). *Physics World*. Retrieved 2023-04-01.
36. Conover, Emily (2023-02-22). "Google's quantum computer reached an error-correcting milestone" (https://www.sciencenews.org/article/google-quantum-computer-sycamore-milestone). *ScienceNews*. Retrieved 2023-04-01.
37. Smith-Goodson, Paul (2024-04-18). "Microsoft And Quantinuum Improve Quantum Error Rates By 800x" (https://www.forbes.com/sites/moorinsights/2024/04/18/microsoft-and-quantinuum-improve-quantum-error-rates-by-800x/). *Forbes*. Retrieved 2024-07-01.
38. Yirka, Bob (2024-04-05). "Quantinuum quantum computer using Microsoft's 'logical quantum bits' runs 14,000 experiments with no errors" (https://phys.org/news/2024-04-quantinuum-quantum-microsoft-logical-bits.html). *Phys.org*. Retrieved 2024-07-01.

39. Ahsan, Muhammad; Naqvi, Syed Abbas Zilqurnain; Anwer, Haider (2022-02-18). "Quantum circuit engineering for correcting coherent noise". *Physical Review A*. **105** (2): 022428. arXiv:2109.03533 (https://arxiv.org/abs/2109.03533). Bibcode:2022PhRvA.105b2428A (https://ui.adsabs.harvard.edu/abs/2022PhRvA.105b2428A). doi:10.1103/physreva.105.022428 (https://doi.org/10.1103%2Fphysreva.105.022428). ISSN 2469-9926 (https://search.worldcat.org/issn/2469-9926). S2CID 237442177 (https://api.semanticscholar.org/CorpusID:237442177).
40. Steffen, Matthias (2022-10-20). "What's the difference between error suppression, error mitigation, and error correction?" (https://research.ibm.com/blog/quantum-error-suppression-mitigation-correction). *IBM Research Blog*. Retrieved 2022-11-26.

Further reading

- Daniel Lidar and Todd Brun, ed. (2013). *Quantum Error Correction*. Cambridge University Press.
- La Guardia, Giuliano Gadioli, ed. (2020). *Quantum Error Correction: Symmetric, Asymmetric, Synchronizable, and Convolutional Codes*. Springer Nature.
- Frank Gaitan (2008). *Quantum Error Correction and Fault Tolerant Quantum Computing*. Taylor & Francis.
- Freedman, Michael H.; Meyer, David A.; Luo, Feng (2002). "Z_2-Systolic freedom and quantum codes". *Mathematics of quantum computation*. Comput. Math. Ser. Boca Raton, FL: Chapman & Hall/CRC. pp. 287–320.
- Freedman, Michael H.; Meyer, David A. (1998). "Projective plane and planar quantum codes". *Found. Comput. Math*. **2001** (3): 325–332. arXiv:quant-ph/9810055 (https://arxiv.org/abs/quant-ph/9810055). Bibcode:1998quant.ph.10055F (https://ui.adsabs.harvard.edu/abs/1998quant.ph.10055F).

External links

- "Topological Quantum Error Correction" (https://www.youtube.com/watch?v=OU9_mrxLl3g). *Quantum Light*. University of Sheffield. 2018-09-28. Archived (https://ghostarchive.org/varchive/youtube/20211222/OU9_mrxLl3g) from the original on 2021-12-22 – via YouTube.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_error_correction&oldid=1241142387"

WIKIPEDIA
The Free Encyclopedia

Bacon–Shor code

The **Bacon–Shor code** is a subsystem error correcting code.[1] In a subsystem code, information is encoded in a subsystem of a Hilbert space. Subsystem codes lend to simplified error correcting procedures unlike codes which encode information in the subspace of a Hilbert space.[2] This simplicity led to the first claim of fault tolerant circuit demonstration on a quantum computer.[3] It is named after Dave Bacon and Peter Shor.

Given the stabilizer generators of Shor's code: $\langle X_0X_1X_2X_3X_4X_5, X_0X_1X_2X_6X_7X_8, Z_0Z_1, Z_1Z_2, Z_3Z_4, Z_4Z_5, Z_6Z_7, Z_7Z_8\rangle$, 4 stabilizers can be removed from this generator by recognizing gauge symmetries in the code to get: $\langle X_0X_1X_2X_3X_4X_5, X_0X_1X_2X_6X_7X_8, Z_0Z_1Z_3Z_4Z_6Z_7, Z_1Z_2Z_4Z_5Z_7Z_8\rangle$.[4] Error correction is now simplified because 4 stabilizers are needed to measure errors instead of 8. A gauge group can be created from the stabilizer generators: $\langle Z_1Z_2, X_2X_8, Z_4Z_5, X_5X_8, Z_0Z_1, X_0X_6, Z_3Z_4, X_3X_6, X_1X_7, X_4X_7, Z_6Z_7, Z_7Z_8\rangle$.[4] Given that the Bacon–Shor code is defined on a square lattice where the qubits are placed on the vertices; laying the qubits on a grid in a way that corresponds to the gauge group shows how only 2 qubit nearest-neighbor measurements are needed to infer the error syndromes. The simplicity of deducing the syndromes reduces the overheard for fault tolerant error correction.[5]



See also

- Five-qubit error correcting code

References

1. Bacon, Dave (2006-01-30). "Operator quantum error-correcting subsystems for self-correcting quantum memories". *Physical Review A*. **73** (1): 012340. arXiv:quant-ph/0506023 (https://arxiv.org/abs/quant-ph/0506023). Bibcode:2006PhRvA..73a2340B (https://ui.adsabs.harvard.edu/abs/2006PhRvA..73a2340B). doi:10.1103/PhysRevA.73.012340 (https://doi.org/10.1103%2FPhysRevA.73.012340). S2CID 118968017 (https://api.semanticscholar.org/CorpusID:118968017).
2. Aly Salah A., Klappenecker, Andreas (2008). "Subsystem code constructions". *2008 IEEE International Symposium on Information Theory*. pp. 369–373. arXiv:0712.4321 (https://arxiv.org/abs/0712.4321). doi:10.1109/ISIT.2008.4595010 (https://doi.org/10.1109%2FISIT.200

8.4595010). ISBN 978-1-4244-2256-2. S2CID 14063318 (https://api.semanticscholar.org/CorpusID:14063318).

3. Egan, L., Debroy, D.M., Noel, C. (2021). "Fault-tolerant control of an error-corrected qubit". *Phys. Rev. Lett*. **598** (7880). Nature: 281–286. arXiv:2009.11482 (https://arxiv.org/abs/2009.11482). Bibcode:2021Natur.598..281E (https://ui.adsabs.harvard.edu/abs/2021Natur.598..281E). doi:10.1038/s41586-021-03928-y (https://doi.org/10.1038%2Fs41586-021-03928-y). PMID 34608286 (https://pubmed.ncbi.nlm.nih.gov/34608286). S2CID 238357892 (https://api.semanticscholar.org/CorpusID:238357892).
4. Poulin, David (2005). "Stabilizer Formalism for Operator Quantum Error Correction" (https://link.aps.org/doi/10.1103/PhysRevLett.95.230504). *Phys. Rev. Lett*. **95** (23). American Physical Society: 230504. arXiv:quant-ph/0508131 (https://arxiv.org/abs/quant-ph/0508131). Bibcode:2005PhRvL..95w0504P (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95w0504P). doi:10.1103/PhysRevLett.95.230504 (https://doi.org/10.1103%2FPhysRevLett.95.230504). PMID 16384287 (https://pubmed.ncbi.nlm.nih.gov/16384287). S2CID 5348507 (https://api.semanticscholar.org/CorpusID:5348507).
5. Aliferis, Panos, Cross, Andrew W. (2007). "Subsystem fault tolerance with the Bacon-Shor code" (https://link.aps.org/doi/10.1103/PhysRevLett.98.220502). *Phys. Rev. Lett*. **98** (22). American Physical Society: 220502. arXiv:quant-ph/0610063 (https://arxiv.org/abs/quant-ph/0610063). Bibcode:2007PhRvL..98v0502A (https://ui.adsabs.harvard.edu/abs/2007PhRvL..98v0502A). doi:10.1103/PhysRevLett.98.220502 (https://doi.org/10.1103%2FPhysRevLett.98.220502). PMID 17677825 (https://pubmed.ncbi.nlm.nih.gov/17677825). S2CID 11002341 (https://api.semanticscholar.org/CorpusID:11002341).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Bacon–Shor_code&oldid=1210539620"

WIKIPEDIA
The Free Encyclopedia

Steane code

The **Steane code** is a tool in quantum error correction introduced by Andrew Steane in 1996. It is a CSS code (Calderbank-Shor-Steane), using the classical binary [7,4,3] Hamming code to correct for both qubit flip errors (X errors) and phase flip errors (Z errors). The Steane code encodes one logical qubit in 7 physical qubits and is able to correct arbitrary single qubit errors.

Its check matrix in standard form is

$$\begin{bmatrix} H & 0 \\ 0 & H \end{bmatrix}$$

where H is the parity-check matrix of the Hamming code and is given by

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

The $[[7, 1, 3]]$ Steane code is the first in the family of quantum Hamming codes, codes with parameters $[[2^r - 1, 2^r - 1 - 2r, 3]]$ for integers $r \geq 3$. It is also a quantum color code.

Expression in the stabilizer formalism

In a quantum error-correcting code, the codespace is the subspace of the overall Hilbert space where all logical states live. In an n-qubit stabilizer code, we can describe this subspace by its Pauli stabilizing group, the set of all n-qubit Pauli operators which stabilize every logical state. The stabilizer formalism allows us to define the codespace of a stabilizer code by specifying its Pauli stabilizing group. We can efficiently describe this exponentially large group by listing its generators.

Since the Steane code encodes one logical qubit in 7 physical qubits, the codespace for the Steane code is a 2-dimensional subspace of its 2^7-dimensional Hilbert space.

In the stabilizer formalism, the Steane code has 6 generators:

$$\begin{aligned} &IIIXXXX \\ &IXXIIXX \\ &XIXIXIX \\ &IIIZZZZ \\ &IZZIIZZ \\ &ZIZIZIZ. \end{aligned}$$

Note that each of the above generators is the tensor product of 7 single-qubit Pauli operations. For instance, $IIIXXXX$ is just shorthand for $I \otimes I \otimes I \otimes X \otimes X \otimes X \otimes X$, that is, an identity on the first three qubits and an X gate on each of the last four qubits. The tensor products are often omitted in

notation for brevity.

The logical X and Z gates are

$$X_L = XXXXXXX$$
$$Z_L = ZZZZZZZ.$$

The logical $|0\rangle$ and $|1\rangle$ states of the Steane code are

$$\begin{aligned}|0\rangle_L =& \frac{1}{\sqrt{8}}[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle] \\ |1\rangle_L =& X_L|0\rangle_L.\end{aligned}$$

Arbitrary codestates are of the form $|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$.

References

- Steane, Andrew (1996). "Multiple-Particle Interference and Quantum Error Correction". *Proc. R. Soc. Lond. A*. **452** (1954): 2551–2577. arXiv:quant-ph/9601029 (https://arxiv.org/abs/quant-ph/9601029). Bibcode:1996RSPSA.452.2551S (https://ui.adsabs.harvard.edu/abs/1996RSPSA.452.2551S). doi:10.1098/rspa.1996.0136 (https://doi.org/10.1098%2Frspa.1996.0136). S2CID 8246615 (https://api.semanticscholar.org/CorpusID:8246615).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Steane_code&oldid=1221445652"

WIKIPEDIA
The Free Encyclopedia

Toric code

The **toric code** is a topological quantum error correcting code, and an example of a stabilizer code, defined on a two-dimensional spin lattice.[1] It is the simplest and most well studied of the quantum double models.[2] It is also the simplest example of topological order—Z_2 topological order (first studied in the context of Z_2 spin liquid in 1991).[3][4] The toric code can also be considered to be a Z_2 lattice gauge theory in a particular limit.[5] It was introduced by Alexei Kitaev.

The toric code gets its name from its periodic boundary conditions, giving it the shape of a torus. These conditions give the model translational invariance, which is useful for analytic study. However, some experimental realizations require open boundary conditions, allowing the system to be embedded on a 2D surface. The resulting code is typically known as the planar code. This has identical behaviour to the toric code in most, but not all, cases.

Error correction and computation

The toric code is defined on a two-dimensional lattice, usually chosen to be the square lattice, with a spin-½ degree of freedom located on each edge. They are chosen to be periodic. Stabilizer operators are defined on the spins around each vertex v and plaquette (or face i.e. a vertex of the dual lattice) p of the lattice as follows,

$$A_v = \prod_{i \in v} \sigma_i^x, \; B_p = \prod_{i \in p} \sigma_i^z.$$

Where here we use $i \in v$ to denote the edges touching the vertex v, and $i \in p$ to denote the edges surrounding the plaquette p. The stabilizer space of the code is that for which all stabilizers act trivially, hence for any state $|\psi\rangle$ in this space it holds that

$$A_v|\psi\rangle = |\psi\rangle, \; \forall v, \; B_p|\psi\rangle = |\psi\rangle, \; \forall p.$$

For the toric code, this space is four-dimensional, and so can be used to store two qubits of quantum information. This can be proven by considering the number of independent stabilizer operators. The occurrence of errors will move the state out of the stabilizer space, resulting in vertices and plaquettes for which the above condition does not hold. The positions of these violations is the syndrome of the code, which can be used for error correction.

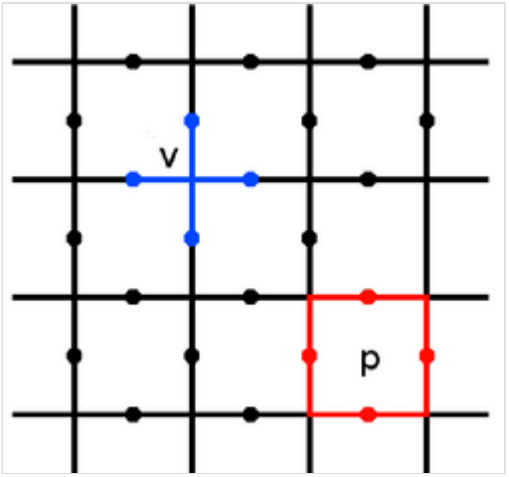
The unique nature of the topological codes, such as the toric code, is that stabilizer violations can be interpreted as quasiparticles. Specifically, if the code is in a state $|\phi\rangle$ such that,

$$A_v|\phi\rangle = -|\phi\rangle,$$

a quasiparticle known as an e anyon can be said to exist on the vertex v. Similarly violations of the B_p are associated with so called m anyons on the plaquettes. The stabilizer space therefore corresponds to the anyonic vacuum. Single spin errors cause pairs of anyons to be created and transported around the

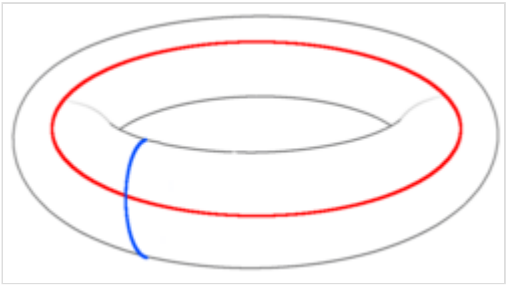
lattice.

When errors create an anyon pair and move the anyons, one can imagine a path connecting the two composed of all links acted upon. If the anyons then meet and are annihilated, this path describes a loop. If the loop is topologically trivial, it has no effect on the stored information. The annihilation of the anyons, in this case, corrects all of the errors involved in their creation and transport. However, if the loop is topologically non-trivial, though re-annihilation of the anyons returns the state to the stabilizer space, it also implements a logical operation on the stored information. The errors, in this case, are therefore not corrected but consolidated.



A section of the toric code. A vertex and plaquette are highlighted, along with the spins used in the definition of their stabilizers.

Consider the noise model for which bit and phase errors occur independently on each spin, both with probability p. When p is low, this will create sparsely distributed pairs of anyons which have not moved far from their point of creation. Correction can be achieved by identifying the pairs that the anyons were created in (up to an equivalence class), and then re-annihilating them to remove the errors. As p increases, however, it becomes more ambiguous as to how the anyons may be paired without risking the formation of topologically non-trivial loops. This gives a threshold probability, under which the error correction will almost certainly succeed. Through a mapping to the random-bond Ising model, this critical probability has been found to be around 11%.[6]


The topologically nontrivial loops of the torus. Moving anyons along these implement logical Pauli operators on the stored qubits.

Other error models may also be considered, and thresholds found. In all cases studied so far, the code has been found to saturate the Hashing bound. For some error models, such as biased errors where bit errors occur more often than phase errors or vice versa, lattices other than the square lattice must be used to achieve the optimal thresholds.[7][8]

These thresholds are upper limits and are useless unless efficient algorithms are found to achieve them. The most well-used algorithm is minimum weight perfect matching.[9] When applied to the noise model with independent bit and flip errors, a threshold of around 10.5% is achieved. This falls only a little short of the 11% maximum. However, matching does not work so well when there are correlations between the bit and phase errors, such as with depolarizing noise.

The means to perform quantum computation on logical information stored within the toric code has been considered, with the properties of the code providing fault-tolerance. It has been shown that extending the stabilizer space using 'holes', vertices or plaquettes on which stabilizers are not enforced, allows many qubits to be encoded into the code. However, a universal set of unitary gates cannot be fault-tolerantly implemented by unitary operations and so additional techniques are required to achieve quantum computing. For example, universal quantum computing can be achieved by preparing magic states via encoded quantum stubs called tidBits used to teleport in the required additional gates when replaced as a qubit. Furthermore, preparation of magic states must be fault tolerant, which can be achieved by magic

state distillation on noisy magic states. A measurement based scheme for quantum computation based upon this principle has been found, whose error threshold is the highest known for a two-dimensional architecture.[10][11]

Hamiltonian and self-correction

Since the stabilizer operators of the toric code are quasilocal, acting only on spins located near each other on a two-dimensional lattice, it is not unrealistic to define the following Hamiltonian,

$$H_{\mathrm{TC}} = -J\sum_{v} A_v - J\sum_{p} B_p, \;\; J > 0.$$

The ground state space of this Hamiltonian is the stabilizer space of the code. Excited states correspond to those of anyons, with the energy proportional to their number. Local errors are therefore energetically suppressed by the gap, which has been shown to be stable against local perturbations.[12] However, the dynamic effects of such perturbations can still cause problems for the code.[13][14]

The gap also gives the code a certain resilience against thermal errors, allowing it to be correctable almost surely for a certain critical time. This time increases with J, but since arbitrary increases of this coupling are unrealistic, the protection given by the Hamiltonian still has its limits.

The means to make the toric code, or the planar code, into a fully self-correcting quantum memory is often considered. Self-correction means that the Hamiltonian will naturally suppress errors indefinitely, leading to a lifetime that diverges in the thermodynamic limit. It has been found that this is possible in the toric code only if long range interactions are present between anyons.[15][16] Proposals have been made for realization of these in the lab [17] Another approach is the generalization of the model to higher dimensions, with self-correction possible in 4D with only quasi-local interactions.[18]

Anyon model

As mentioned above, so called e and m quasiparticles are associated with the vertices and plaquettes of the model, respectively. These quasiparticles can be described as anyons, due to the non-trivial effect of their braiding. Specifically, though both species of anyons are bosonic with respect to themselves, the braiding of two e's or m's having no effect, a full monodromy of an e and an m will yield a phase of -1. Such a result is not consistent with either bosonic or fermionic statistics, and hence is anyonic.

The anyonic mutual statistics of the quasiparticles demonstrate the logical operations performed by topologically non-trivial loops. Consider the creation of a pair of e anyons followed by the transport of one around a topologically nontrivial loop, such as that shown on the torus in blue on the figure above, before the pair are reannhilated. The state is returned to the stabilizer space, but the loop implements a logical operation on one of the stored qubits. If m anyons are similarly moved through the red loop above a logical operation will also result. The phase of -1 resulting when braiding the anyons shows that these operations do not commute, but rather anticommute. They may therefore be interpreted as logical Z and X Pauli operators on one of the stored qubits. The corresponding logical Pauli's on the other qubit correspond to an m anyon following the blue loop and an e anyon following the red. No braiding occurs

when e and m pass through parallel paths, the phase of -1 therefore does not arise and the corresponding logical operations commute. This is as should be expected since these form operations acting on different qubits.

Due to the fact that both e and m anyons can be created in pairs, it is clear to see that both these quasiparticles are their own antiparticles. A composite particle composed of two e anyons is therefore equivalent to the vacuum, since the vacuum can yield such a pair and such a pair will annihilate to the vacuum. Accordingly, these composites have bosonic statistics, since their braiding is always completely trivial. A composite of two m anyons is similarly equivalent to the vacuum. The creation of such composites is known as the fusion of anyons, and the results can be written in terms of fusion rules. In this case, these take the form,

$$e \times e = 1, \;\; m \times m = 1.$$

Where 1 denotes the vacuum. A composite of an e and an m is not trivial. This therefore constitutes another quasiparticle in the model, sometimes denoted ψ, with fusion rule,

$$e \times m = \psi.$$

From the braiding statistics of the anyons we see that, since any single exchange of two ψ's will involve a full monodromy of a constituent e and m, a phase of -1 will result. This implies fermionic self-statistics for the ψ's.

Generalizations

The use of a torus is not required to form an error correcting code. Other surfaces may also be used, with their topological properties determining the degeneracy of the stabilizer space. In general, quantum error correcting codes defined on two-dimensional spin lattices according to the principles above are known as surface codes.[19]

It is also possible to define similar codes using higher-dimensional spins. These are the quantum double models[20] and string-net models,[21] which allow a greater richness in the behaviour of anyons, and so may be used for more advanced quantum computation and error correction proposals.[22] These not only include models with Abelian anyons, but also those with non-Abelian statistics.[23][24][25]

Experimental progress

The most explicit demonstration of the properties of the toric code has been in state based approaches. Rather than attempting to realize the Hamiltonian, these simply prepare the code in the stabilizer space. Using this technique, experiments have been able to demonstrate the creation, transport and statistics of the anyons[26][27][28] and measurement of the topological entanglement entropy.[28] More recent experiments have also been able to demonstrate the error correction properties of the code.[29][28]

For realizations of the toric code and its generalizations with a Hamiltonian, much progress has been made using Josephson junctions. The theory of how the Hamiltonians may be implemented has been developed for a wide class of topological codes.[30] An experiment has also been performed, realizing the

toric code Hamiltonian for a small lattice, and demonstrating the quantum memory provided by its degenerate ground state.[31]

Other theoretical and experimental works towards realizations are based on cold atoms. A toolkit of methods that may be used to realize topological codes with optical lattices has been explored, [32] as have experiments concerning minimal instances of topological order.[33] Such minimal instances of the toric code has been realized experimentally within isolated square plaquettes.[34] Progress is also being made into simulations of the toric model with Rydberg atoms, in which the Hamiltonian and the effects of dissipative noise can be demonstrated.[35][36] Experiments in Rydberg atom arrays have also successfully realized the toric code with periodic boundary conditions in two dimensions by coherently transporting arrays of entangled atoms.[37]

References

1. A. Y. Kitaev, Proceedings of the 3rd International Conference of Quantum Communication and Measurement, Ed. O. Hirota, A. S. Holevo, and C. M. Caves (New York, Plenum, 1997)
2. Kitaev, Alexei (2006). "Anyons in an exactly solved model and beyond". *Annals of Physics*. **321** (1): 2–111. arXiv:cond-mat/0506438 (https://arxiv.org/abs/cond-mat/0506438). Bibcode:2006AnPhy.321....2K (https://ui.adsabs.harvard.edu/abs/2006AnPhy.321....2K). doi:10.1016/j.aop.2005.10.005 (https://doi.org/10.1016%2Fj.aop.2005.10.005). ISSN 0003-4916 (https://search.worldcat.org/issn/0003-4916). S2CID 118948929 (https://api.semanticscholar.org/CorpusID:118948929).
3. Read, N.; Sachdev, Subir (1 March 1991). "Large-Nexpansion for frustrated quantum antiferromagnets". *Physical Review Letters*. **66** (13): 1773–1776. Bibcode:1991PhRvL..66.1773R (https://ui.adsabs.harvard.edu/abs/1991PhRvL..66.1773R). doi:10.1103/physrevlett.66.1773 (https://doi.org/10.1103%2Fphysrevlett.66.1773). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10043303 (https://pubmed.ncbi.nlm.nih.gov/10043303).
4. Wen, X. G. (1 July 1991). "Mean-field theory of spin-liquid states with finite energy gap and topological orders". *Physical Review B*. **44** (6): 2664–2672. Bibcode:1991PhRvB..44.2664W (https://ui.adsabs.harvard.edu/abs/1991PhRvB..44.2664W). doi:10.1103/physrevb.44.2664 (https://doi.org/10.1103%2Fphysrevb.44.2664). ISSN 0163-1829 (https://search.worldcat.org/issn/0163-1829). PMID 9999836 (https://pubmed.ncbi.nlm.nih.gov/9999836).
5. Fradkin, Eduardo; Shenker, Stephen H. (15 June 1979). "Phase diagrams of lattice gauge theories with Higgs fields". *Physical Review D*. **19** (12): 3682–3697. Bibcode:1979PhRvD..19.3682F (https://ui.adsabs.harvard.edu/abs/1979PhRvD..19.3682F). doi:10.1103/physrevd.19.3682 (https://doi.org/10.1103%2Fphysrevd.19.3682). ISSN 0556-2821 (https://search.worldcat.org/issn/0556-2821).
6. Dennis, Eric; Kitaev, Alexei; Landahl, Andrew; Preskill, John (2002). "Topological quantum memory". *Journal of Mathematical Physics*. **43** (9): 4452–4505. arXiv:quant-ph/0110143 (https://arxiv.org/abs/quant-ph/0110143). Bibcode:2002JMP....43.4452D (https://ui.adsabs.harvard.edu/abs/2002JMP....43.4452D). doi:10.1063/1.1499754 (https://doi.org/10.1063%2F1.1499754). ISSN 0022-2488 (https://search.worldcat.org/issn/0022-2488). S2CID 36673677 (https://api.semanticscholar.org/CorpusID:36673677).

7. Röthlisberger, Beat; Wootton, James R.; Heath, Robert M.; Pachos, Jiannis K.; Loss, Daniel (13 February 2012). "Incoherent dynamics in the toric code subject to disorder". *Physical Review A*. **85** (2): 022313. arXiv:1112.1613 (https://arxiv.org/abs/1112.1613). Bibcode:2012PhRvA..85b2313R (https://ui.adsabs.harvard.edu/abs/2012PhRvA..85b2313R). doi:10.1103/physreva.85.022313 (https://doi.org/10.1103%2Fphysreva.85.022313). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 118585279 (https://api.semanticscholar.org/CorpusID:118585279).
8. Bombin, H.; Andrist, Ruben S.; Ohzeki, Masayuki; Katzgraber, Helmut G.; Martin-Delgado, M. A. (30 April 2012). "Strong Resilience of Topological Codes to Depolarization" (https://doi.org/10.1103%2Fphysrevx.2.021004). *Physical Review X*. **2** (2): 021004. arXiv:1202.1852 (https://arxiv.org/abs/1202.1852). Bibcode:2012PhRvX...2b1004B (https://ui.adsabs.harvard.edu/abs/2012PhRvX...2b1004B). doi:10.1103/physrevx.2.021004 (https://doi.org/10.1103%2Fphysrevx.2.021004). ISSN 2160-3308 (https://search.worldcat.org/issn/2160-3308).
9. Edmonds, Jack (1965). "Paths, Trees, and Flowers" (https://doi.org/10.4153%2Fcjm-1965-045-4). *Canadian Journal of Mathematics*. **17**: 449–467. doi:10.4153/cjm-1965-045-4 (https://doi.org/10.4153%2Fcjm-1965-045-4). ISSN 0008-414X (https://search.worldcat.org/issn/0008-414X). S2CID 247198603 (https://api.semanticscholar.org/CorpusID:247198603).
10. Raussendorf, Robert; Harrington, Jim (11 May 2007). "Fault-Tolerant Quantum Computation with High Threshold in Two Dimensions". *Physical Review Letters*. **98** (19): 190504. arXiv:quant-ph/0610082 (https://arxiv.org/abs/quant-ph/0610082). Bibcode:2007PhRvL..98s0504R (https://ui.adsabs.harvard.edu/abs/2007PhRvL..98s0504R). doi:10.1103/physrevlett.98.190504 (https://doi.org/10.1103%2Fphysrevlett.98.190504). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 17677613 (https://pubmed.ncbi.nlm.nih.gov/17677613). S2CID 39504821 (https://api.semanticscholar.org/CorpusID:39504821).
11. Raussendorf, R; Harrington, J; Goyal, K (29 June 2007). "Topological fault-tolerance in cluster state quantum computation" (https://doi.org/10.1088%2F1367-2630%2F9%2F6%2F199). *New Journal of Physics*. **9** (6): 199. arXiv:quant-ph/0703143 (https://arxiv.org/abs/quant-ph/0703143). Bibcode:2007NJPh....9..199R (https://ui.adsabs.harvard.edu/abs/2007NJPh....9..199R). doi:10.1088/1367-2630/9/6/199 (https://doi.org/10.1088%2F1367-2630%2F9%2F6%2F199). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).
12. Bravyi, Sergey; Hastings, Matthew B.; Michalakis, Spyridon (2010). "Topological quantum order: Stability under local perturbations". *Journal of Mathematical Physics*. **51** (9): 093512. arXiv:1001.0344 (https://arxiv.org/abs/1001.0344). Bibcode:2010JMP....51i3512B (https://ui.adsabs.harvard.edu/abs/2010JMP....51i3512B). doi:10.1063/1.3490195 (https://doi.org/10.1063%2F1.3490195). ISSN 0022-2488 (https://search.worldcat.org/issn/0022-2488). S2CID 115166306 (https://api.semanticscholar.org/CorpusID:115166306).
13. F. Pastawski; A. Kay; N. Schuch; J. I. Cirac (2010). "Limitations of passive protection of quantum information". *Quantum Information and Computation*. **10** (7&8): 580. arXiv:0911.3843 (https://arxiv.org/abs/0911.3843). doi:10.26421/qic10.7-8 (https://doi.org/10.26421%2Fqic10.7-8). ISSN 1533-7146 (https://search.worldcat.org/issn/1533-7146). S2CID 3076085 (https://api.semanticscholar.org/CorpusID:3076085).
14. Freeman, C. Daniel; Herdman, C. M.; Gorman, D. J.; Whaley, K. B. (7 October 2014). "Relaxation dynamics of the toric code in contact with a thermal reservoir: Finite-size scaling in a low-temperature regime". *Physical Review B*. **90** (13): 134302. arXiv:1405.2315 (https://arxiv.org/abs/1405.2315). Bibcode:2014PhRvB..90m4302F (https://ui.adsabs.harvard.edu/abs/2014PhRvB..90m4302F). doi:10.1103/physrevb.90.134302 (https://doi.org/10.1103%2Fphysrevb.90.134302). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 118724410 (https://api.semanticscholar.org/CorpusID:118724410).

15. Hamma, Alioscia; Castelnovo, Claudio; Chamon, Claudio (18 June 2009). "Toric-boson model: Toward a topological quantum memory at finite temperature". *Physical Review B*. **79** (24): 245122. arXiv:0812.4622 (https://arxiv.org/abs/0812.4622). Bibcode:2009PhRvB..79x5122H (https://ui.adsabs.harvard.edu/abs/2009PhRvB..79x5122H). doi:10.1103/physrevb.79.245122 (https://doi.org/10.1103%2Fphysrevb.79.245122). hdl:1721.1/51820 (https://hdl.handle.net/1721.1%2F51820). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 5202832 (https://api.semanticscholar.org/CorpusID:5202832).
16. Chesi, Stefano; Röthlisberger, Beat; Loss, Daniel (6 August 2010). "Self-correcting quantum memory in a thermal environment". *Physical Review A*. **82** (2): 022305. arXiv:0908.4264 (https://arxiv.org/abs/0908.4264). Bibcode:2010PhRvA..82b2305C (https://ui.adsabs.harvard.edu/abs/2010PhRvA..82b2305C). doi:10.1103/physreva.82.022305 (https://doi.org/10.1103%2Fphysreva.82.022305). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 118400202 (https://api.semanticscholar.org/CorpusID:118400202).
17. Pedrocchi, Fabio L.; Chesi, Stefano; Loss, Daniel (10 March 2011). "Quantum memory coupled to cavity modes". *Physical Review B*. **83** (11): 115415. arXiv:1011.3762 (https://arxiv.org/abs/1011.3762). Bibcode:2011PhRvB..83k5415P (https://ui.adsabs.harvard.edu/abs/2011PhRvB..83k5415P). doi:10.1103/physrevb.83.115415 (https://doi.org/10.1103%2Fphysrevb.83.115415). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 118595257 (https://api.semanticscholar.org/CorpusID:118595257).
18. Alicki, R.; Horodecki, M.; Horodecki, P.; Horodecki, R. (2010). "On Thermal Stability of Topological Qubit in Kitaev's 4D Model". *Open Systems & Information Dynamics*. **17** (1): 1–20. arXiv:0811.0033 (https://arxiv.org/abs/0811.0033). doi:10.1142/s1230161210000023 (https://doi.org/10.1142%2Fs1230161210000023). ISSN 1230-1612 (https://search.worldcat.org/issn/1230-1612). S2CID 26719502 (https://api.semanticscholar.org/CorpusID:26719502).
19. Ghosh, Joydip; Fowler, Austin G.; Geller, Michael R. (19 December 2012). "Surface code with decoherence: An analysis of three superconducting architectures". *Physical Review A*. **86** (6): 062318. arXiv:1210.5799 (https://arxiv.org/abs/1210.5799). Bibcode:2012PhRvA..86f2318G (https://ui.adsabs.harvard.edu/abs/2012PhRvA..86f2318G). doi:10.1103/physreva.86.062318 (https://doi.org/10.1103%2Fphysreva.86.062318). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 10196488 (https://api.semanticscholar.org/CorpusID:10196488).
20. Bullock, Stephen S; Brennen, Gavin K (14 March 2007). "Qudit surface codes and gauge theory with finite cyclic groups". *Journal of Physics A: Mathematical and Theoretical*. **40** (13): 3481–3505. arXiv:quant-ph/0609070 (https://arxiv.org/abs/quant-ph/0609070). Bibcode:2007JPhA...40.3481B (https://ui.adsabs.harvard.edu/abs/2007JPhA...40.3481B). doi:10.1088/1751-8113/40/13/013 (https://doi.org/10.1088%2F1751-8113%2F40%2F13%2F013). ISSN 1751-8113 (https://search.worldcat.org/issn/1751-8113). S2CID 15630224 (https://api.semanticscholar.org/CorpusID:15630224).
21. Levin, Michael A. and Xiao-Gang Wen (12 January 2005). "String-net condensation: A physical mechanism for topological phases". *Physical Review B*. **71** (45110): 21. arXiv:cond-mat/0404617 (https://arxiv.org/abs/cond-mat/0404617). Bibcode:2005PhRvB..71d5110L (https://ui.adsabs.harvard.edu/abs/2005PhRvB..71d5110L). doi:10.1103/PhysRevB.71.045110 (https://doi.org/10.1103%2FPhysRevB.71.045110). S2CID 51962817 (https://api.semanticscholar.org/CorpusID:51962817).
22. Wootton, James R.; Lahtinen, Ville; Doucot, Benoit; Pachos, Jiannis K. (2011). "Engineering complex topological memories from simple Abelian models". *Annals of Physics*. **326** (9): 2307–2314. arXiv:0908.0708 (https://arxiv.org/abs/0908.0708). Bibcode:2011AnPhy.326.2307W (https://ui.adsabs.harvard.edu/abs/2011AnPhy.326.2307W). doi:10.1016/j.aop.2011.05.008 (https://doi.org/10.1016%2Fj.aop.2011.05.008). ISSN 0003-4916 (https://search.worldcat.org/issn/0003-4916). S2CID 119288871 (https://api.semanticscholar.org/CorpusID:119288871).

23. Aguado, M.; Brennen, G. K.; Verstraete, F.; Cirac, J. I. (22 December 2008). "Creation, Manipulation, and Detection of Abelian and Non-Abelian Anyons in Optical Lattices". *Physical Review Letters*. **101** (26): 260501. arXiv:0802.3163 (https://arxiv.org/abs/0802.3163). Bibcode:2008PhRvL.101z0501A (https://ui.adsabs.harvard.edu/abs/2008PhRvL.101z0501A). doi:10.1103/physrevlett.101.260501 (https://doi.org/10.1103%2Fphysrevlett.101.260501). hdl:1854/LU-8589252 (https://hdl.handle.net/1854%2FLU-8589252). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 19113760 (https://pubmed.ncbi.nlm.nih.gov/19113760). S2CID 11619038 (https://api.semanticscholar.org/CorpusID:11619038).
24. Brennen, G K; Aguado, M; Cirac, J I (22 May 2009). "Simulations of quantum double models" (https://doi.org/10.1088%2F1367-2630%2F11%2F5%2F053009). *New Journal of Physics*. **11** (5): 053009. arXiv:0901.1345 (https://arxiv.org/abs/0901.1345). Bibcode:2009NJPh...11e3009B (https://ui.adsabs.harvard.edu/abs/2009NJPh...11e3009B). doi:10.1088/1367-2630/11/5/053009 (https://doi.org/10.1088%2F1367-2630%2F11%2F5%2F053009). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).
25. Liu, Yu-Jie; Shtengel, Kirill; Smith, Adam; Pollmann, Frank (2022-11-07). "Methods for Simulating String-Net States and Anyons on a Digital Quantum Computer" (https://link.aps.org/doi/10.1103/PRXQuantum.3.040315). *PRX Quantum*. **3** (4): 040315. arXiv:2110.02020 (https://arxiv.org/abs/2110.02020). Bibcode:2022PRXQ....3d0315L (https://ui.adsabs.harvard.edu/abs/2022PRXQ....3d0315L). doi:10.1103/PRXQuantum.3.040315 (https://doi.org/10.1103%2FPRXQuantum.3.040315). S2CID 238353914 (https://api.semanticscholar.org/CorpusID:238353914).
26. Pachos, J K; Wieczorek, W; Schmid, C; Kiesel, N; Pohlner, R; Weinfurter, H (12 August 2009). "Revealing anyonic features in a toric code quantum simulation" (https://doi.org/10.1088%2F1367-2630%2F11%2F8%2F083010). *New Journal of Physics*. **11** (8): 083010. arXiv:0710.0895 (https://arxiv.org/abs/0710.0895). Bibcode:2009NJPh...11h3010P (https://ui.adsabs.harvard.edu/abs/2009NJPh...11h3010P). doi:10.1088/1367-2630/11/8/083010 (https://doi.org/10.1088%2F1367-2630%2F11%2F8%2F083010). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630).
27. C.-Y. Lu, et al., Phys. Rev. Lett. **102**, 030502 (2009).
28. Satzinger, K. J.; Liu, Y.; Smith, A.; Knapp, C.; Newman, M.; Jones, C.; Chen, Z.; Quintana, C.; Mi, X.; Dunsworth, A.; Gidney, C. (2021-04-02). "Realizing topologically ordered states on a quantum processor". *Science*. **374** (6572): 1237–1241. arXiv:2104.01180 (https://arxiv.org/abs/2104.01180). Bibcode:2021Sci...374.1237S (https://ui.adsabs.harvard.edu/abs/2021Sci...374.1237S). doi:10.1126/science.abi8378 (https://doi.org/10.1126%2Fscience.abi8378). PMID 34855491 (https://pubmed.ncbi.nlm.nih.gov/34855491). S2CID 233025160 (https://api.semanticscholar.org/CorpusID:233025160).
29. Yao, Xing-Can; Wang, Tian-Xiong; Chen, Hao-Ze; Gao, Wei-Bo; Fowler, Austin G.; Raussendorf, Robert; Chen, Zeng-Bing; Liu, Nai-Le; Lu, Chao-Yang; Deng, You-Jin; Chen, Yu-Ao; Pan, Jian-Wei (22 February 2012). "Experimental demonstration of topological error correction". *Nature*. **482** (7386): 489–494. arXiv:0905.1542 (https://arxiv.org/abs/0905.1542). Bibcode:2012Natur.482..489Y (https://ui.adsabs.harvard.edu/abs/2012Natur.482..489Y). doi:10.1038/nature10770 (https://doi.org/10.1038%2Fnature10770). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 22358838 (https://pubmed.ncbi.nlm.nih.gov/22358838). S2CID 4307662 (https://api.semanticscholar.org/CorpusID:4307662).
30. Douçot, Benoit; Ioffe, Lev B.; Vidal, Julien (3 June 2004). "Discrete non-Abelian gauge theories in Josephson-junction arrays and quantum computation". *Physical Review B*. **69** (21): 214501. arXiv:cond-mat/0302104 (https://arxiv.org/abs/cond-mat/0302104). Bibcode:2004PhRvB..69u4501D (https://ui.adsabs.harvard.edu/abs/2004PhRvB..69u4501D). doi:10.1103/physrevb.69.214501 (https://doi.org/10.1103%2Fphysrevb.69.214501). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 119407144 (https://api.semanticscholar.org/CorpusID:119407144).

31. Gladchenko, Sergey; Olaya, David; Dupont-Ferrier, Eva; Douçot, Benoit; Ioffe, Lev B.; Gershenson, Michael E. (2009). "Superconducting nanocircuits for topologically protected qubits". *Nature Physics*. **5** (1): 48–53. arXiv:0802.2295 (https://arxiv.org/abs/0802.2295). Bibcode:2009NatPh...5...48G (https://ui.adsabs.harvard.edu/abs/2009NatPh...5...48G). doi:10.1038/nphys1151 (https://doi.org/10.1038%2Fnphys1151). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 118359424 (https://api.semanticscholar.org/CorpusID:118359424).
32. Micheli, A.; Brennen, G. K.; Zoller, P. (30 April 2006). "A toolbox for lattice-spin models with polar molecules". *Nature Physics*. **2** (5): 341–347. arXiv:quant-ph/0512222 (https://arxiv.org/abs/quant-ph/0512222). Bibcode:2006NatPh...2..341M (https://ui.adsabs.harvard.edu/abs/2006NatPh...2..341M). doi:10.1038/nphys287 (https://doi.org/10.1038%2Fnphys287). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 108289844 (https://api.semanticscholar.org/CorpusID:108289844).
33. Paredes, Belén; Bloch, Immanuel (1 January 2008). "Minimum instances of topological matter in an optical plaquette". *Physical Review A*. **77** (2): 023603. arXiv:0711.3796 (https://arxiv.org/abs/0711.3796). Bibcode:2008PhRvA..77b3603P (https://ui.adsabs.harvard.edu/abs/2008PhRvA..77b3603P). doi:10.1103/physreva.77.023603 (https://doi.org/10.1103%2Fphysreva.77.023603). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 46143303 (https://api.semanticscholar.org/CorpusID:46143303).
34. Dai, Hanning; Yang, Bing; Reingruber, Andreas; Sun, Hui; Xu, Xiao-Fan; Chen, Yu-Ao; Yuan, Zhen-Sheng; Pan, Jian-Wei (28 August 2017). "Four-body ring-exchange interactions and anyonic statistics within a minimal toric-code Hamiltonian". *Nature Physics*. **13** (2): 1195–1200. arXiv:1602.05709 (https://arxiv.org/abs/1602.05709). Bibcode:2017NatPh..13.1195D (https://ui.adsabs.harvard.edu/abs/2017NatPh..13.1195D). doi:10.1038/NPHYS4243 (https://doi.org/10.1038%2FNPHYS4243). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 118604118 (https://api.semanticscholar.org/CorpusID:118604118).
35. Weimer, Hendrik; Müller, Markus; Lesanovsky, Igor; Zoller, Peter; Büchler, Hans Peter (14 March 2010). "A Rydberg quantum simulator". *Nature Physics*. **6** (5): 382–388. arXiv:0907.1657 (https://arxiv.org/abs/0907.1657). Bibcode:2010NatPh...6..382W (https://ui.adsabs.harvard.edu/abs/2010NatPh...6..382W). doi:10.1038/nphys1614 (https://doi.org/10.1038%2Fnphys1614). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 54710282 (https://api.semanticscholar.org/CorpusID:54710282).
36. Semeghini, Giulia; Levine, Harry; Keesling, Alexander; Ebadi, Sepehr; Wang, Tout T.; Bluvstein, Dolev; Verresen, Ruben; Pichler, Hannes; Kalinowski, Marcin; Samajdar, Rhine; Omran, Ahmed (2021). "Probing Topological Spin Liquids on a Programmable Quantum Simulator". *Science*. **374** (6572): 1242–1247. arXiv:2104.04119 (https://arxiv.org/abs/2104.04119). Bibcode:2021Sci...374.1242S (https://ui.adsabs.harvard.edu/abs/2021Sci...374.1242S). doi:10.1126/science.abi8794 (https://doi.org/10.1126%2Fscience.abi8794). PMID 34855494 (https://pubmed.ncbi.nlm.nih.gov/34855494). S2CID 233204440 (https://api.semanticscholar.org/CorpusID:233204440).
37. Bluvstein, Dolev; Levine, Harry; Semeghini, Giulia; Wang, Tout; Ebadi, Sepehr; Kalinowski, Marcin; Maskara, Nishad; Pichler, Hannes; Greiner, Marcus; Vuletic, Vladan; Lukin, Misha (April 20, 2022). "A quantum processor based on coherent transport of entangled atom arrays" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9021024). *Nature*. **604** (7906): 451–456. arXiv:2112.03923 (https://arxiv.org/abs/2112.03923). Bibcode:2022Natur.604..451B (https://ui.adsabs.harvard.edu/abs/2022Natur.604..451B). doi:10.1038/s41586-022-04592-6 (https://doi.org/10.1038%2Fs41586-022-04592-6). PMC 9021024 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9021024). PMID 35444318 (https://pubmed.ncbi.nlm.nih.gov/35444318). S2CID 244954259 (https://api.semanticscholar.org/CorpusID:244954259).

External links

- https://skepsisfera.blogspot.com/2010/04/kitaevs-toric-code.html

---

Retrieved from "https://en.wikipedia.org/w/index.php?title=Toric_code&oldid=1193558626"

WIKIPEDIA
The Free Encyclopedia

gnu code

In quantum information, the ***gnu* code** refers to a particular family of quantum error correcting codes, with the special property of being invariant under permutations of the qubits. Given integers *g* (the *gap*), *n* (the occupancy), and *m* (the length of the code), the two codewords are

$$|0_{\mathrm{L}}\rangle = \sum_{\substack{\ell \text{ even} \\ 0 \le \ell \le n}} \sqrt{\frac{\binom{n}{\ell}}{2^{n-1}}} |D^m_{g\ell}\rangle$$

$$|1_{\mathrm{L}}\rangle = \sum_{\substack{\ell \text{ odd} \\ 0 \le \ell \le n}} \sqrt{\frac{\binom{n}{\ell}}{2^{n-1}}} |D^m_{g\ell}\rangle$$

where $|D^m_k\rangle$ are the Dicke states consisting of a uniform superposition of all weight-*k* words on *m* qubits, e.g.

$$|D^4_2\rangle = \frac{|0011\rangle + |0101\rangle + |1001\rangle + |0110\rangle + |1010\rangle + |1100\rangle}{\sqrt{6}}$$

The real parameter $u = \dfrac{m}{gn}$ scales the density of the code. The length $m = gnu$, hence the name of the code. For odd $g = n$ and $u \geq 1$, the *gnu* code is capable of correcting $\dfrac{g-1}{2}$ erasure errors,[1] or deletion errors.[2]

References

1. Ouyang, Yingkai (2014-12-10). "Permutation-invariant quantum codes". *Physical Review A*. **90** (6): 062317. arXiv:1302.3247 (https://arxiv.org/abs/1302.3247). Bibcode:2014PhRvA..90f2317O (https://ui.adsabs.harvard.edu/abs/2014PhRvA..90f2317O). doi:10.1103/physreva.90.062317 (https://doi.org/10.1103%2Fphysreva.90.062317). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 119114455 (https://api.semanticscholar.org/CorpusID:119114455).
2. Ouyang, Yingkai (2021-02-04). "Permutation-invariant quantum coding for quantum deletion channels". arXiv:2102.02494v1 (https://arxiv.org/abs/2102.02494v1) [quant-ph (https://arxiv.org/archive/quant-ph)].

Retrieved from "https://en.wikipedia.org/w/index.php?title=Gnu_code&oldid=1178842307"

WIKIPEDIA
The Free Encyclopedia

Entanglement-assisted stabilizer formalism

In the theory of quantum communication, the **entanglement-assisted stabilizer formalism** is a method for protecting quantum information with the help of entanglement shared between a sender and receiver before they transmit quantum data over a quantum communication channel. It extends the standard stabilizer formalism by including shared entanglement (Brun *et al.* 2006). The advantage of entanglement-assisted stabilizer codes is that the sender can exploit the error-correcting properties of an arbitrary set of Pauli operators. The sender's Pauli operators do not necessarily have to form an Abelian subgroup of the Pauli group Π^n over n qubits. The sender can make clever use of her shared ebits so that the global stabilizer is Abelian and thus forms a valid quantum error-correcting code.

Definition

We review the construction of an entanglement-assisted code (Brun *et al.* 2006). Suppose that there is a nonabelian subgroup $\mathcal{S} \subset \Pi^n$ of size $n-k = 2c+s$. Application of the fundamental theorem of symplectic geometry (Lemma 1 in the first external reference) states that there exists a minimal set of independent generators $\left\{\bar{Z}_1, \ldots, \bar{Z}_{s+c}, \bar{X}_{s+1}, \ldots, \bar{X}_{s+c}\right\}$ for $\mathcal{S}$ with the following commutation relations:

$$\begin{aligned}
\left[\bar{Z}_i, \bar{Z}_j\right] &= 0 \quad \forall i,j, \\
\left[\bar{X}_i, \bar{X}_j\right] &= 0 \quad \forall i,j, \\
\left[\bar{X}_i, \bar{Z}_j\right] &= 0 \quad \forall i \neq j, \\
\left\{\bar{X}_i, \bar{Z}_i\right\} &= 0 \quad \forall i.
\end{aligned}$$

The decomposition of $\mathcal{S}$ into the above minimal generating set determines that the code requires s ancilla qubits and c ebits. The code requires an ebit for every anticommuting pair in the minimal generating set. The simple reason for this requirement is that an ebit is a simultaneous $+1$-eigenstate of the Pauli operators $\{XX, ZZ\}$. The second qubit in the ebit transforms the anticommuting pair $\{X, Z\}$ into a commuting pair $\{XX, ZZ\}$. The above decomposition also minimizes the number of ebits required for the code---it is an optimal decomposition.

We can partition the nonabelian group $\mathcal{S}$ into two subgroups: the isotropic subgroup $\mathcal{S}_I$ and the entanglement subgroup $\mathcal{S}_E$. The isotropic subgroup $\mathcal{S}_I$ is a commuting subgroup of $\mathcal{S}$ and thus corresponds to ancilla qubits:

$$\mathcal{S}_I = \left\{\bar{Z}_1, \ldots, \bar{Z}_s\right\}.$$

The elements of the entanglement subgroup $\mathcal{S}_E$ come in anticommuting pairs and thus correspond to ebits:

$$\mathcal{S}_E = \left\{ \bar{Z}_{s+1}, \ldots, \bar{Z}_{s+c}, \bar{X}_{s+1}, \ldots, \bar{X}_{s+c} \right\}.$$

Entanglement-assisted stabilizer code error correction conditions

The two subgroups $\mathcal{S}_I$ and $\mathcal{S}_E$ play a role in the error-correcting conditions for the entanglement-assisted stabilizer formalism. An entanglement-assisted code corrects errors in a set $\mathcal{E} \subset \Pi^n$ if for all $E_1, E_2 \in \mathcal{E}$,

$$E_1^\dagger E_2 \in \mathcal{S}_I \cup \left(\Pi^n - \mathcal{Z}\left(\langle \mathcal{S}_I, \mathcal{S}_E \rangle \right) \right).$$

Operation

The operation of an entanglement-assisted code is as follows. The sender performs an encoding unitary on her unprotected qubits, ancilla qubits, and her half of the ebits. The unencoded state is a simultaneous +1-eigenstate of the following Pauli operators:

$$\{ Z_1, \ldots, Z_s, Z_{s+1} | Z_1, \ldots, Z_{s+c} | Z_c, X_{s+1} | X_1, \ldots, X_{s+c} | X_c \}.$$

The Pauli operators to the right of the vertical bars indicate the receiver's half of the shared ebits. The encoding unitary transforms the unencoded Pauli operators to the following encoded Pauli operators:

$$\left\{ \bar{Z}_1, \ldots, \bar{Z}_s, \bar{Z}_{s+1} | Z_1, \ldots, \bar{Z}_{s+c} | Z_c, \bar{X}_{s+1} | X_1, \ldots, \bar{X}_{s+c} | X_c \right\}.$$

The sender transmits all of her qubits over the noisy quantum channel. The receiver then possesses the transmitted qubits and his half of the ebits. He measures the above encoded operators to diagnose the error. The last step is to correct the error.

Rate of an entanglement-assisted code

We can interpret the rate of an entanglement-assisted code in three different ways (Wilde and Brun 2007b). Suppose that an entanglement-assisted quantum code encodes k information qubits into n physical qubits with the help of c ebits.

- The *entanglement-assisted* rate assumes that entanglement shared between sender and receiver is free. Bennett et al. make this assumption when deriving the entanglement assisted capacity of a quantum channel for sending quantum information. The entanglement-assisted rate is k/n for a code with the above parameters.
- The *trade-off* rate assumes that entanglement is not free and a rate pair determines performance. The first number in the pair is the number of noiseless qubits generated per channel use, and the second number in the pair is the number of ebits consumed per channel use. The rate pair is $(k/n, c/n)$ for a code with the above parameters. Quantum information theorists have computed asymptotic trade-off curves that bound the rate region in which achievable rate pairs lie. The construction for an entanglement-assisted quantum block code minimizes the number c of ebits given a fixed number k and n of respective information qubits and physical qubits.

- The *catalytic rate* assumes that bits of entanglement are built up at the expense of transmitted qubits. A noiseless quantum channel or the encoded use of noisy quantum channel are two different ways to build up entanglement between a sender and receiver. The catalytic rate of an $[n, k; c]$ code is $(k - c)/n$.

Which interpretation is most reasonable depends on the context in which we use the code. In any case, the parameters n, k, and c ultimately govern performance, regardless of which definition of the rate we use to interpret that performance.

Example of an entanglement-assisted code

We present an example of an entanglement-assisted code that corrects an arbitrary single-qubit error (Brun *et al*. 2006). Suppose the sender wants to use the quantum error-correcting properties of the following nonabelian subgroup of Π^4:

$$\begin{array}{cccc} Z & X & Z & I \\ Z & Z & I & Z \\ X & Y & X & I \\ X & X & I & X \end{array}$$

The first two generators anticommute. We obtain a modified third generator by multiplying the third generator by the second. We then multiply the last generator by the first, second, and modified third generators. The error-correcting properties of the generators are invariant under these operations. The modified generators are as follows:

$$\begin{array}{cccccc} g_1 & = & Z & X & Z & I \\ g_2 & = & Z & Z & I & Z \\ g_3 & = & Y & X & X & Z \\ g_4 & = & Z & Y & Y & X \end{array}$$

The above set of generators have the commutation relations given by the fundamental theorem of symplectic geometry:

$$\{g_1, g_2\} = [g_1, g_3] = [g_1, g_4] = [g_2, g_3] = [g_2, g_4] = [g_3, g_4] = 0.$$

The above set of generators is unitarily equivalent to the following canonical generators:

$$\begin{array}{cccc} X & I & I & I \\ Z & I & I & I \\ I & Z & I & I \\ I & I & Z & I \end{array}$$

We can add one ebit to resolve the anticommutativity of the first two generators and obtain the canonical stabilizer:

$$\begin{array}{c|cccc} X & X & I & I & I \\ Z & Z & I & I & I \\ I & I & Z & I & I \\ I & I & I & Z & I \end{array}$$

The receiver Bob possesses the qubit on the left and the sender Alice possesses the four qubits on the right. The following state is an eigenstate of the above stabilizer

$$|\Phi^{+}\rangle^{BA}|00\rangle^{A}|\psi\rangle^{A}.$$

where $|\psi\rangle^{A}$ is a qubit that the sender wants to encode. The encoding unitary then rotates the canonical stabilizer to the following set of globally commuting generators:

$$\begin{array}{c|cccc} X & Z & X & Z & I \\ Z & Z & Z & I & Z \\ I & Y & X & X & Z \\ I & Z & Y & Y & X \end{array}$$

The receiver measures the above generators upon receipt of all qubits to detect and correct errors.

Encoding algorithm

We continue with the previous example. We detail an algorithm for determining an encoding circuit and the optimal number of ebits for the entanglement-assisted code---this algorithm first appeared in the appendix of (Wilde and Brun 2007a) and later in the appendix of (Shaw *et al.* 2008). The operators in the above example have the following representation as a binary matrix (See the stabilizer code article):

$$H = \left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

Call the matrix to the left of the vertical bar the "Z matrix" and the matrix to the right of the vertical bar the "X matrix."

The algorithm consists of row and column operations on the above matrix. Row operations do not affect the error-correcting properties of the code but are crucial for arriving at the optimal decomposition from the fundamental theorem of symplectic geometry. The operations available for manipulating columns of the above matrix are Clifford operations. Clifford operations preserve the Pauli group Π^{n} under conjugation. The CNOT gate, the Hadamard gate, and the Phase gate generate the Clifford group. A CNOT gate from qubit i to qubit j adds column i to column j in the X matrix and adds column j to column i in the Z matrix. A Hadamard gate on qubit i swaps column i in the Z matrix with column i in the X matrix and vice versa. A phase gate on qubit i adds column i in the X matrix to column i in the Z matrix. Three CNOT gates implement a qubit swap operation. The effect of a swap on qubits i and j is to swap columns i and j in both the X and Z matrix.

The algorithm begins by computing the symplectic product between the first row and all other rows. We emphasize that the symplectic product here is the standard symplectic product. Leave the matrix as it is if the first row is not symplectically orthogonal to the second row or if the first row is symplectically orthogonal to all other rows. Otherwise, swap the second row with the first available row that is not symplectically orthogonal to the first row. In our example, the first row is not symplectically orthogonal to the second so we leave all rows as they are.

Arrange the first row so that the top left entry in the X matrix is one. A CNOT, swap, Hadamard, or combinations of these operations can achieve this result. We can have this result in our example by swapping qubits one and two. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

Perform CNOTs to clear the entries in the X matrix in the top row to the right of the leftmost entry. These entries are already zero in this example so we need not do anything. Proceed to the clear the entries in the first row of the Z matrix. Perform a phase gate to clear the leftmost entry in the first row of the Z matrix if it is equal to one. It is equal to zero in this case so we need not do anything. We then use Hadamards and CNOTs to clear the other entries in the first row of the Z matrix.

We perform the above operations for our example. Perform a Hadamard on qubits two and three. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right].$$

Perform a CNOT from qubit one to qubit two and from qubit one to qubit three. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

The first row is complete. We now proceed to clear the entries in the second row. Perform a Hadamard on qubits one and four. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right].$$

Perform a CNOT from qubit one to qubit two and from qubit one to qubit four. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right].$$

The first two rows are now complete. They need one ebit to compensate for their anticommutativity or their nonorthogonality with respect to the symplectic product.

Now we perform a "Gram-Schmidt orthogonalization" with respect to the symplectic product. Add row one to any other row that has one as the leftmost entry in its Z matrix. Add row two to any other row that has one as the leftmost entry in its X matrix. For our example, we add row one to row four and we add row two to rows three and four. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right].$$

The first two rows are now symplectically orthogonal to all other rows per the fundamental theorem of symplectic geometry. We proceed with the same algorithm on the next two rows. The next two rows are symplectically orthogonal to each other so we can deal with them individually. Perform a Hadamard on qubit two. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right].$$

Perform a CNOT from qubit two to qubit three and from qubit two to qubit four. The matrix becomes

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right].$$

Perform a phase gate on qubit two:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right].$$

Perform a Hadamard on qubit three followed by a CNOT from qubit two to qubit three:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right].$$

Add row three to row four and perform a Hadamard on qubit two:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{array}\right].$$

Perform a Hadamard on qubit four followed by a CNOT from qubit three to qubit four. End by performing a Hadamard on qubit three:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right].$$

The above matrix now corresponds to the canonical Pauli operators. Adding one half of an ebit to the receiver's side gives the canonical stabilizer whose simultaneous +1-eigenstate is the above state. The above operations in reverse order take the canonical stabilizer to the encoded stabilizer.

References

- Brun, T.; Devetak, I.; Hsieh, M.-H. (2006-10-20). "Correcting Quantum Errors with Entanglement". *Science*. **314** (5798). American Association for the Advancement of Science (AAAS): 436–439. arXiv:quant-ph/0610092 (https://arxiv.org/abs/quant-ph/0610092). Bibcode:2006Sci...314..436B (https://ui.adsabs.harvard.edu/abs/2006Sci...314..436B). doi:10.1126/science.1131563 (https://doi.org/10.1126%2Fscience.1131563). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 17008489 (https://pubmed.ncbi.nlm.nih.gov/17008489). S2CID 18106089 (https://api.semanticscholar.org/CorpusID:18106089).
- Min-Hsiu Hsieh. *Entanglement-assisted Coding Theory.* Ph.D. Dissertation, University of Southern California, August 2008. Available at https://arxiv.org/abs/0807.2080
- Mark M. Wilde. *Quantum Coding with Entanglement.* Ph.D. Dissertation, University of Southern California, August 2008. Available at https://arxiv.org/abs/0806.4214
- Hsieh, Min-Hsiu; Devetak, Igor; Brun, Todd (2007-12-19). "General entanglement-assisted quantum error-correcting codes". *Physical Review A*. **76** (6): 062313. arXiv:0708.2142 (https://arxiv.org/abs/0708.2142). Bibcode:2007PhRvA..76f2313H (https://ui.adsabs.harvard.edu/abs/2007PhRvA..76f2313H). doi:10.1103/physreva.76.062313 (https://doi.org/10.1103%2Fphysreva.76.062313). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 119155178 (https://api.semanticscholar.org/CorpusID:119155178).
- Kremsky, Isaac; Hsieh, Min-Hsiu; Brun, Todd A. (2008-07-21). "Classical enhancement of quantum-error-correcting codes". *Physical Review A*. **78** (1): 012341. arXiv:0802.2414 (https://arxiv.org/abs/0802.2414). Bibcode:2008PhRvA..78a2341K (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78a2341K). doi:10.1103/physreva.78.012341 (https://doi.org/10.1103%2

Fphysreva.78.012341). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 119252610 (https://api.semanticscholar.org/CorpusID:119252610).

- Wilde, Mark M.; Brun, Todd A. (2008-06-19). "Optimal entanglement formulas for entanglement-assisted quantum coding". *Physical Review A*. **77** (6): 064302. arXiv:0804.1404 (https://arxiv.org/abs/0804.1404). Bibcode:2008PhRvA..77f4302W (https://ui.adsabs.harvard.edu/abs/2008PhRvA..77f4302W). doi:10.1103/physreva.77.064302 (https://doi.org/10.1103%2Fphysreva.77.064302). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 118411793 (https://api.semanticscholar.org/CorpusID:118411793).
- Wilde, Mark M.; Krovi, Hari; Brun, Todd A. (2010). "Convolutional entanglement distillation". *2010 IEEE International Symposium on Information Theory*. IEEE. pp. 2657–2661. arXiv:0708.3699 (https://arxiv.org/abs/0708.3699). doi:10.1109/isit.2010.5513666 (https://doi.org/10.1109%2Fisit.2010.5513666). ISBN 978-1-4244-7892-7.
- Wilde, Mark M.; Brun, Todd A. (2010-04-30). "Entanglement-assisted quantum convolutional coding". *Physical Review A*. **81** (4): 042333. arXiv:0712.2223 (https://arxiv.org/abs/0712.2223). Bibcode:2010PhRvA..81d2333W (https://ui.adsabs.harvard.edu/abs/2010PhRvA..81d2333W). doi:10.1103/physreva.81.042333 (https://doi.org/10.1103%2Fphysreva.81.042333). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 8410654 (https://api.semanticscholar.org/CorpusID:8410654).
- Wilde, Mark M.; Brun, Todd A. (2010-06-08). "Quantum convolutional coding with shared entanglement: general structure". *Quantum Information Processing*. **9** (5). Springer Science and Business Media LLC: 509–540. arXiv:0807.3803 (https://arxiv.org/abs/0807.3803). doi:10.1007/s11128-010-0179-9 (https://doi.org/10.1007%2Fs11128-010-0179-9). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 18185704 (https://api.semanticscholar.org/CorpusID:18185704).
- Shaw, Bilal; Wilde, Mark M.; Oreshkov, Ognyan; Kremsky, Isaac; Lidar, Daniel A. (2008-07-18). "Encoding one logical qubit into six physical qubits". *Physical Review A*. **78** (1): 012337. arXiv:0803.1495 (https://arxiv.org/abs/0803.1495). Bibcode:2008PhRvA..78a2337S (https://ui.adsabs.harvard.edu/abs/2008PhRvA..78a2337S). doi:10.1103/physreva.78.012337 (https://doi.org/10.1103%2Fphysreva.78.012337). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 40040752 (https://api.semanticscholar.org/CorpusID:40040752).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Entanglement-assisted_stabilizer_formalism&oldid=1190319474"

WIKIPEDIA
The Free Encyclopedia

Quantum optics

Quantum optics is a branch of atomic, molecular, and optical physics dealing with how individual quanta of light, known as photons, interact with atoms and molecules. It includes the study of the particle-like properties of photons. Photons have been used to test many of the counter-intuitive predictions of quantum mechanics, such as entanglement and teleportation, and are a useful resource for quantum information processing.

History

Light propagating in a restricted volume of space has its energy and momentum quantized according to an integer number of particles known as photons. Quantum optics studies the nature and effects of light as quantized photons. The first major development leading to that understanding was the correct modeling of the blackbody radiation spectrum by Max Planck in 1899 under the hypothesis of light being emitted in discrete units of energy. The photoelectric effect was further evidence of this quantization as explained by Albert Einstein in a 1905 paper, a discovery for which he was to be awarded the Nobel Prize in 1921. Niels Bohr showed that the hypothesis of optical radiation being quantized corresponded to his theory of the quantized energy levels of atoms, and the spectrum of discharge emission from hydrogen in particular. The understanding of the interaction between light and matter following these developments was crucial for the development of quantum mechanics as a whole. However, the subfields of quantum mechanics dealing with matter-light interaction were principally regarded as research into matter rather than into light; hence one rather spoke of atom physics and quantum electronics in 1960. Laser science—i.e., research into principles, design and application of these devices—became an important field, and the quantum mechanics underlying the laser's principles was studied now with more emphasis on the properties of light, and the name *quantum optics* became customary.

As laser science needed good theoretical foundations, and also because research into these soon proved very fruitful, interest in quantum optics rose. Following the work of Dirac in quantum field theory, John R. Klauder, George Sudarshan, Roy J. Glauber, and Leonard Mandel applied quantum theory to the electromagnetic field in the 1950s and 1960s to gain a more detailed understanding of photodetection and the statistics of light (see degree of coherence). This led to the introduction of the coherent state as a concept that addressed variations between laser light, thermal light, exotic squeezed states, etc. as it became understood that light cannot be fully described just referring to the electromagnetic fields describing the waves in the classical picture. In 1977, Kimble et al. demonstrated a single atom emitting one photon at a time, further compelling evidence that light consists of photons. Previously unknown quantum states of light with characteristics unlike classical states, such as squeezed light were subsequently discovered.

Development of short and ultrashort laser pulses—created by Q switching and modelocking techniques—opened the way to the study of what became known as ultrafast processes. Applications for solid state research (e.g. Raman spectroscopy) were found, and mechanical forces of light on matter were studied.

The latter led to levitating and positioning clouds of atoms or even small biological samples in an optical trap or optical tweezers by laser beam. This, along with Doppler cooling and Sisyphus cooling, was the crucial technology needed to achieve the celebrated Bose–Einstein condensation.

Other remarkable results are the demonstration of quantum entanglement, quantum teleportation, and quantum logic gates. The latter are of much interest in quantum information theory, a subject that partly emerged from quantum optics, partly from theoretical computer science.[1]

Today's fields of interest among quantum optics researchers include parametric down-conversion, parametric oscillation, even shorter (attosecond) light pulses, use of quantum optics for quantum information, manipulation of single atoms, Bose–Einstein condensates, their application, and how to manipulate them (a sub-field often called atom optics), coherent perfect absorbers, and much more. Topics classified under the term of quantum optics, especially as applied to engineering and technological innovation, often go under the modern term photonics.

Several Nobel prizes have been awarded for work in quantum optics. These were awarded:

- in 2022, Alain Aspect, John Clauser and Anton Zeilinger "for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science".[2]
- in 2012, Serge Haroche and David J. Wineland "for ground-breaking experimental methods that enable measuring & manipulation of individual quantum systems".[3]
- in 2005, Theodor W. Hänsch, Roy J. Glauber and John L. Hall[4]
- in 2001, Wolfgang Ketterle, Eric Allin Cornell and Carl Wieman[5]
- in 1997, Steven Chu, Claude Cohen-Tannoudji and William Daniel Phillips[6]

Concepts

According to quantum theory, light may be considered not only to be as an electro-magnetic wave but also as a "stream" of particles called photons, which travel with *c*, the speed of light in vacuum. These particles should not be considered to be classical billiard balls, but as quantum mechanical particles described by a wavefunction spread over a finite region.

Each particle carries one quantum of energy, equal to *hf*, where *h* is the Planck constant and *f* is the frequency of the light. That energy possessed by a single photon corresponds exactly to the transition between discrete energy levels in an atom (or other system) that emitted the photon; material absorption of a photon is the reverse process. Einstein's explanation of spontaneous emission also predicted the existence of stimulated emission, the principle upon which the laser rests. However, the actual invention of the maser (and laser) many years later was dependent on a method to produce a population inversion.

The use of statistical mechanics is fundamental to the concepts of quantum optics: light is described in terms of field operators for creation and annihilation of photons—i.e. in the language of quantum electrodynamics.

A frequently encountered state of the light field is the coherent state, as introduced by E.C. George Sudarshan in 1960. This state, which can be used to approximately describe the output of a single-frequency laser well above the laser threshold, exhibits Poissonian photon number statistics. Via certain nonlinear interactions, a coherent state can be transformed into a squeezed coherent state, by applying a

squeezing operator that can exhibit super- or sub-Poissonian photon statistics. Such light is called squeezed light. Other important quantum aspects are related to correlations of photon statistics between different beams. For example, spontaneous parametric down-conversion can generate so-called 'twin beams', where (ideally) each photon of one beam is associated with a photon in the other beam.

Atoms are considered as quantum mechanical oscillators with a discrete energy spectrum, with the transitions between the energy eigenstates being driven by the absorption or emission of light according to Einstein's theory.

For solid state matter, one uses the energy band models of solid state physics. This is important for understanding how light is detected by solid-state devices, commonly used in experiments.

Quantum electronics

Quantum electronics is a term that was used mainly between the 1950s and 1970s[7] to denote the area of physics dealing with the effects of quantum mechanics on the behavior of electrons in matter, together with their interactions with photons. Today, it is rarely considered a sub-field in its own right, and it has been absorbed by other fields. Solid state physics regularly takes quantum mechanics into account, and is usually concerned with electrons. Specific applications of quantum mechanics in electronics is researched within semiconductor physics. The term also encompassed the basic processes of laser operation, which is today studied as a topic in quantum optics. Usage of the term overlapped early work on the quantum Hall effect and quantum cellular automata.

See also



Physics portal

- Atomic, molecular, and optical physics
- Attophysics
- Nonclassical light
- Optomechanics
- Quantum control
- Optical phase space
- Optical physics
- Optics
- Quantization of the electromagnetic field
- Two-state quantum system
- Spinplasmonics
- Valleytronics

Notes

1. Nielsen, Michael A.; Chuang, Isaac L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge: Cambridge University Press. ISBN 978-1107002173.
2. "The Nobel Prize in Physics 2022" (https://www.nobelprize.org/prizes/physics/2022/summary/). Nobel Foundation. Retrieved 9 June 2023.
3. "The Nobel Prize in Physics 2012" (https://www.nobelprize.org/nobel_prizes/physics/laureates/2012/index.html). Nobel Foundation. Retrieved 9 October 2012.
4. "The Nobel Prize in Physics 2005" (https://www.nobelprize.org/nobel_prizes/physics/laureates/2005/). Nobelprize.org. Retrieved 2015-10-14.

5. "The Nobel Prize in Physics 2001" (https://www.nobelprize.org/nobel_prizes/physics/laureates/2001/). Nobelprize.org. Retrieved 2015-10-14.
6. "The Nobel Prize in Physics 1997" (https://www.nobelprize.org/nobel_prizes/physics/laureates/1997/). Nobelprize.org. Retrieved 2015-10-14.
7. Brunner, Witlof; Radloff, Wolfgang; Junge, Klaus (1975). *Quantenelektronik* (in German). Deutscher Verlag der Wissenschaften.

References

- Gerry, Christopher; Knight, Peter (2004). *Introduction to Quantum Optics*. Cambridge University Press. ISBN 052152735X.
- The Nobel Prize in Physics 2005 (https://www.nobelprize.org/nobel_prizes/physics/laureates/2005/)

Further reading

- L. Mandel, E. Wolf *Optical Coherence and Quantum Optics* (Cambridge 1995).
- D. F. Walls and G. J. Milburn *Quantum Optics* (Springer 1994).
- Crispin Gardiner and Peter Zoller, *Quantum Noise* (Springer 2004).
- H.M. Moya-Cessa and F. Soto-Eguibar, *Introduction to Quantum Optics* (Rinton Press 2011).
- M. O. Scully and M. S. Zubairy *Quantum Optics* (Cambridge 1997).
- W. P. Schleich *Quantum Optics in Phase Space* (Wiley 2001).
- Kira, M.; Koch, S. W. (2011). *Semiconductor Quantum Optics*. Cambridge University Press. ISBN 978-0521875097.
- F. J. Duarte (2014). *Quantum Optics for Engineers*. New York: CRC. ISBN 978-1439888537.

External links

- An introduction to quantum optics of the light field (http://gerdbreitenbach.de/gallery)
- Encyclopedia of laser physics and technology (http://www.rp-photonics.com/encyclopedia.html), with content on quantum optics (particularly quantum noise in lasers), by Rüdiger Paschotta.
- Qwiki (https://web.archive.org/web/20090924044639/http://qwiki.stanford.edu/wiki/Quantum_Optics) – a quantum physics wiki devoted to providing technical resources for practicing quantum physicists.
- Quantiki (http://www.quantiki.org/) – a free-content WWW resource in quantum information science that anyone can edit.
- Various Quantum Optics Reports (http://www.physics.drexel.edu/~tim/Decoherence/index.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_optics&oldid=1238269098"

WIKIPEDIA
The Free Encyclopedia

Cavity quantum electrodynamics

Cavity quantum electrodynamics (**cavity QED**) is the study of the interaction between light confined in a reflective cavity and atoms or other particles, under conditions where the quantum nature of photons is significant. It could in principle be used to construct a quantum computer.

The case of a single 2-level atom in the cavity is mathematically described by the Jaynes–Cummings model, and undergoes vacuum Rabi oscillations $|e\rangle|n-1\rangle \leftrightarrow |g\rangle|n\rangle$, that is between an excited atom and $n-1$ photons, and a ground state atom and n photons.

If the cavity is in resonance with the atomic transition, a half-cycle of oscillation starting with no photons coherently swaps the atom qubit's state onto the cavity field's, $(\alpha|g\rangle + \beta|e\rangle)|0\rangle \leftrightarrow |g\rangle(\alpha|0\rangle + \beta|1\rangle)$, and can be repeated to swap it back again; this could be used as a single photon source (starting with an excited atom), or as an interface between an atom or trapped ion quantum computer and optical quantum communication.

Other interaction durations create entanglement between the atom and cavity field; for example, a quarter-cycle on resonance starting from $|e\rangle|0\rangle$ gives the maximally entangled state (a Bell state) $(|e\rangle|0\rangle + |g\rangle|1\rangle)/\sqrt{2}$. This can in principle be used as a quantum computer, mathematically equivalent to a trapped ion quantum computer with cavity photons replacing phonons.

Nobel Prize in Physics

The 2012 Nobel Prize for Physics was awarded to Serge Haroche and David Wineland for their work on controlling quantum systems.[1]

Haroche shares half of the prize for developing a new field called cavity quantum electrodynamics (CQED) – whereby the properties of an atom are controlled by placing it in an optical or microwave cavity. Haroche focused on microwave experiments and turned the technique on its head – using CQED to control the properties of individual photons.[1]

In a series of ground-breaking experiments, Haroche used CQED to realize Schrödinger's famous cat experiment in which a system is in a superposition of two very different quantum states until a measurement is made on the system. Such states are extremely fragile, and the techniques developed to create and measure CQED states are now being applied to the development of quantum computers.

See also

- Circuit quantum electrodynamics
- Superconducting radio frequency

- Dicke model

References

- Herbert Walther; Benjamin T H Varcoe; Berthold-Georg Englert; Thomas Becker (2006). "Cavity quantum electrodynamics" (http://www.iop.org/EJ/abstract/0034-4885/69/5/R02/). *Rep. Prog. Phys*. **69** (5): 1325–1382. Bibcode:2006RPPh...69.1325W (https://ui.adsabs.harvard.edu/abs/2006RPPh...69.1325W). doi:10.1088/0034-4885/69/5/R02 (https://doi.org/10.1088%2F0034-4885%2F69%2F5%2FR02). S2CID 122420445 (https://api.semanticscholar.org/CorpusID:122420445). Microwave wavelengths, atoms passing through cavity
- R Miller; T E Northup; K M Birnbaum; A Boca; A D Boozer; H J Kimble (2005). "Trapped atoms in cavity QED: coupling quantized light and matter" (http://www.iop.org/EJ/abstract/0953-4075/38/9/007/). *J. Phys. B: At. Mol. Opt. Phys*. **38** (9): S551–S565. Bibcode:2005JPhB...38S.551M (https://ui.adsabs.harvard.edu/abs/2005JPhB...38S.551M). doi:10.1088/0953-4075/38/9/007 (https://doi.org/10.1088%2F0953-4075%2F38%2F9%2F007). S2CID 1114899 (https://api.semanticscholar.org/CorpusID:1114899). Optical wavelengths, atoms trapped

1. Johnston, Hamish (9 October 2012). "Quantum-control pioneers bag 2012 Nobel Prize for Physics" (http://physicsworld.com/cws/article/news/2012/oct/09/quantum-control-pioneers-bag-2012-nobel-prize-for-physics). *Physics World*. London. Retrieved 2013-10-09.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cavity_quantum_electrodynamics&oldid=1179600299"

WIKIPEDIA
The Free Encyclopedia

Circuit quantum electrodynamics

Circuit quantum electrodynamics (**circuit QED**) provides a means of studying the fundamental interaction between light and matter (quantum optics).[1] As in the field of cavity quantum electrodynamics, a single photon within a single mode cavity coherently couples to a quantum object (atom). In contrast to cavity QED, the photon is stored in a one-dimensional on-chip resonator and the quantum object is no natural atom but an artificial one. These artificial atoms usually are mesoscopic devices which exhibit an atom-like energy spectrum. The field of circuit QED is a prominent example for quantum information processing and a promising candidate for future quantum computation.[2]

In the late 2010s decade, experiments involving cQED in 3 dimensions have demonstrated deterministic gate teleportation and other operations on multiple qubits.[3][4]

Resonator

The resonant devices used for circuit QED are superconducting coplanar waveguide microwave resonators,[5][6] which are two-dimensional microwave analogues of the Fabry–Pérot interferometer. Coplanar waveguides consist of a signal carrying centerline flanked by two grounded planes. This planar structure is put on a dielectric substrate by a photolithographic process. Superconducting materials used are mostly aluminium (Al) or niobium (Nb). Dielectrics typically used as substrates are either surface oxidized silicon (Si) or sapphire (Al_2O_3). The line impedance is given by the geometric properties, which are chosen to match the 50 Ω of the peripheric microwave equipment to avoid partial reflection of the signal.[7] The electric field is basically confined between the center conductor and the ground planes resulting in a very small mode volume V_m which gives rise to very high electric fields per photon E_0 (compared to three-dimensional cavities). Mathematically, the field E_0 can be found as

$$E_0 = \sqrt{\frac{\hbar\omega_r}{2\varepsilon_0 V_m}},$$

where $\hbar$ is the reduced Planck constant, ω_r is the angular frequency, and ε_0 is the permittivity of free space.

One can distinguish between two different types of resonators: $\lambda/2$ and $\lambda/4$ resonators. Half-wavelength resonators are made by breaking the center conductor at two spots with the distance ℓ. The resulting piece of center conductor is in this way capacitively coupled to the input and output and represents a resonator with E-field antinodes at its ends. Quarter-wavelength resonators are short pieces of a coplanar line, which are shorted to ground on one end and capacitively coupled to a feed line on the other. The resonance frequencies are given by

$$\lambda/2: \quad \nu_n = \frac{c}{\sqrt{\varepsilon_{\text{eff}}}}\frac{n}{2\ell} \quad (n = 1, 2, 3, \ldots) \qquad \lambda/4: \quad \nu_n = \frac{c}{\sqrt{\varepsilon_{\text{eff}}}}\frac{2n+1}{4\ell} \quad (n = 0, 1, 2, \ldots)$$

with ε_{eff} being the effective dielectric permittivity of the device.

Artificial atoms, Qubits

The first realized artificial atom in circuit QED was the so-called Cooper-pair box, also known as the charge qubit.[8] In this device, a reservoir of Cooper pairs is coupled via Josephson junctions to a gated superconducting island. The state of the Cooper-pair box (qubit) is given by the number of Cooper pairs on the island (N Cooper pairs for the ground state $|g\rangle$ and $N+1$ for the excited state $|e\rangle$). By controlling the Coulomb energy (bias voltage) and the Josephson energy (flux bias) the transition frequency ω_a is tuned. Due to the nonlinearity of the Josephson junctions the Cooper-pair box shows an atom like energy spectrum. Other more recent examples for qubits used in circuit QED are so called transmon qubits[9] (more charge noise insensitive compared to the Cooper-pair box) and flux qubits (whose state is given by the direction of a supercurrent in a superconducting loop intersected by Josephson junctions). All of these devices feature very large dipole moments d (up to 10^3 times that of large n Rydberg atoms), which qualifies them as extremely suitable coupling counterparts for the light field in circuit QED.

Theory

The full quantum description of matter-light interaction is given by the Jaynes–Cummings model.[10] The three terms of the Jaynes–Cummings model can be ascribed to a cavity term, which is mimicked by a harmonic oscillator, an atomic term and an interaction term.

$$\mathcal{H}_{\text{JC}} = \underbrace{\hbar\omega_r\left(a^\dagger a + \frac{1}{2}\right)}_{\text{cavity term}} + \underbrace{\frac{1}{2}\hbar\omega_a\sigma_z}_{\text{atomic term}} + \underbrace{\hbar g\left(\sigma_+ a + a^\dagger\sigma_-\right)}_{\text{interaction term}}$$

In this formulation ω_r is the resonance frequency of the cavity and $a^\dagger$ and a are photon creation and annihilation operators, respectively. The atomic term is given by the Hamiltonian of a spin-1/2 system with ω_a being the transition frequency and σ_z the Pauli matrix. The operators $\sigma_\pm$ are raising and lowering operators (ladder operators) for the atomic states. For the case of zero detuning ($\omega_r = \omega_a$) the interaction lifts the degeneracy of the photon number state $|n\rangle$ and the atomic states $|g\rangle$ and $|e\rangle$ and pairs of dressed states are formed. These new states are superpositions of cavity and atom states

$$|n, \pm\rangle = \frac{1}{\sqrt{2}}\left(|g\rangle \mid n\rangle \pm \mid e\rangle \mid n-1\rangle\right)$$

and are energetically split by $2g\sqrt{n}$. If the detuning is significantly larger than the combined cavity and atomic linewidth the cavity states are merely shifted by $\pm g^2/\Delta$ (with the detuning $\Delta = \omega_a - \omega_r$) depending on the atomic state. This provides the possibility to read out the atomic (qubit) state by measuring the transition frequency.

The coupling is given by $g = E \cdot d$ (for electric dipolar coupling). If the coupling is much larger than the cavity loss rate $\kappa = \frac{\omega_r}{Q}$ (quality factor Q; the higher Q, the longer the photon remains inside the resonator) as well as the decoherence rate γ (rate at which the qubit relaxes into modes other than the resonator mode) the strong coupling regime is reached. Due to the high fields and low losses of the coplanar resonators together with the large dipole moments and long decoherence times of the qubits, the strong coupling regime can easily be reached in the field of circuit QED. Combination of the Jaynes–Cummings model and the coupled cavities leads to the Jaynes–Cummings–Hubbard model.

See also

- Superconducting radio frequency

References

1. Schuster, David I. (May 2007). *Circuit Quantum Electrodynamics* (https://rsl.yale.edu/sites/default/files/files/RSL_Theses/SchusterThesis.pdf) (PDF) (PhD thesis). Yale University.
2. Alexandre Blais; et al. (2004). "Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computing". *Phys. Rev. A*. **69** (6): 062320. arXiv:cond-mat/0402216 (https://arxiv.org/abs/cond-mat/0402216). Bibcode:2004PhRvA..69f2320B (https://ui.adsabs.harvard.edu/abs/2004PhRvA..69f2320B). doi:10.1103/PhysRevA.69.062320 (https://doi.org/10.1103%2FPhysRevA.69.062320). S2CID 20427333 (https://api.semanticscholar.org/CorpusID:20427333).
3. Blumoff, Jacob Z. (December 2017). *Multiqubit experiments in 3D circuit quantum electrodynamics* (https://rsl.yale.edu/sites/default/files/files/RSL_Theses/jzb_thesis_finaldigital_Aug24.pdf) (PDF) (PhD thesis). Yale University.
4. Chou, Kevin S. (May 2018). *Teleported operations between logical qubits in circuit quantum electrodynamics* (https://rsl.yale.edu/sites/default/files/files/kevinchou_thesis_2018.pdf) (PDF) (PhD thesis). Yale University.
5. Luigi Frunzio; et al. (2005). "Fabrication and Characterization of Superconducting Circuit QED Devices for Quantum Computation". *IEEE Transactions on Applied Superconductivity*. **15** (2): 860–863. arXiv:cond-mat/0411708 (https://arxiv.org/abs/cond-mat/0411708). Bibcode:2005ITAS...15..860F (https://ui.adsabs.harvard.edu/abs/2005ITAS...15..860F). doi:10.1109/TASC.2005.850084 (https://doi.org/10.1109%2FTASC.2005.850084). S2CID 12789596 (https://api.semanticscholar.org/CorpusID:12789596).
6. M. Göppl; et al. (2008). "Coplanar waveguide resonators for circuit quantum electrodynamics". *J. Appl. Phys.* **104** (11): 113904–113904–8. arXiv:0807.4094 (https://arxiv.org/abs/0807.4094). Bibcode:2008JAP...104k3904G (https://ui.adsabs.harvard.edu/abs/2008JAP...104k3904G). doi:10.1063/1.3010859 (https://doi.org/10.1063%2F1.3010859). S2CID 56398614 (https://api.semanticscholar.org/CorpusID:56398614).
7. Simons, Rainee N. (2001). *Coplanar Waveguide Circuits, Components, and Systems*. John Wiley & Sons Inc. ISBN 0-471-16121-7.
8. A. Wallraff; et al. (2004). "Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics". *Nature*. **431** (7005). Nature Publishing Group: 162–167. arXiv:cond-mat/0407325 (https://arxiv.org/abs/cond-mat/0407325). Bibcode:2004Natur.431..162W (https://ui.adsabs.harvard.edu/abs/2004Natur.431..162W). doi:10.1038/nature02851 (https://doi.org/10.1038%2Fnature02851). PMID 15356625 (https://pubmed.ncbi.nlm.nih.gov/15356625). S2CID 55812008 (https://api.semanticscholar.org/CorpusID:55812008).

9. Jens Koch; et al. (2007). "Charge insensitive qubit design derived from the Cooper pair box". *Phys. Rev. A*. **76** (4): 042319. arXiv:cond-mat/0703002 (https://arxiv.org/abs/cond-mat/0703002). Bibcode:2007PhRvA..76d2319K (https://ui.adsabs.harvard.edu/abs/2007PhRvA..76d2319K). doi:10.1103/PhysRevA.76.042319 (https://doi.org/10.1103%2FPhysRevA.76.042319). S2CID 53983107 (https://api.semanticscholar.org/CorpusID:53983107).
10. E. T. Jaynes and F. W. Cummings (1963). "Comparison of Quantum and Semiclassical Radiation Theories with Application to the Beam Maser". *Proceedings of the IEEE*. **51**. IEEE: 89–109. doi:10.1109/proc.1963.1664 (https://doi.org/10.1109%2Fproc.1963.1664).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Circuit_quantum_electrodynamics&oldid=1226055628"

WIKIPEDIA
The Free Encyclopedia

Linear optical quantum computing

Linear optical quantum computing or **linear optics quantum computation** (**LOQC**), also **photonic quantum computing (PQC)**, is a paradigm of quantum computation, allowing (under certain conditions, described below) universal quantum computation. LOQC uses photons as information carriers, mainly uses linear optical elements, or optical instruments (including reciprocal mirrors and waveplates) to process quantum information, and uses photon detectors and quantum memories to detect and store quantum information.[1][2][3]

Overview

Although there are many other implementations for quantum information processing (QIP) and quantum computation, optical quantum systems are prominent candidates, since they link quantum computation and quantum communication in the same framework. In optical systems for quantum information processing, the unit of light in a given mode—or photon—is used to represent a qubit. Superpositions of quantum states can be easily represented, encrypted, transmitted and detected using photons. Besides, linear optical elements of optical systems may be the simplest building blocks to realize quantum operations and quantum gates. Each linear optical element equivalently applies a unitary transformation on a finite number of qubits. The system of finite linear optical elements constructs a network of linear optics, which can realize any quantum circuit diagram or quantum network based on the quantum circuit model. Quantum computing with continuous variables is also possible under the linear optics scheme.[4]

The universality of 1- and 2-bit gates to implement arbitrary quantum computation has been proven.[5][6][7][8] Up to $N \times N$ unitary matrix operations ($U(N)$) can be realized by only using mirrors, beam splitters and phase shifters[9] (this is also a starting point of boson sampling and of computational complexity analysis for LOQC). It points out that each $U(N)$ operator with N inputs and N outputs can be constructed via $\mathcal{O}(N^2)$ linear optical elements. Based on the reason of universality and complexity, LOQC usually only uses mirrors, beam splitters, phase shifters and their combinations such as Mach–Zehnder interferometers with phase shifts to implement arbitrary quantum operators. If using a non-deterministic scheme, this fact also implies that LOQC could be resource-inefficient in terms of the number of optical elements and time steps needed to implement a certain quantum gate or circuit, which is a major drawback of LOQC.

Operations via linear optical elements (beam splitters, mirrors and phase shifters, in this case) preserve the photon statistics of input light. For example, a coherent (classical) light input produces a coherent light output; a superposition of quantum states input yields a quantum light state output.[3] Due to this reason, people usually use single photon source case to analyze the effect of linear optical elements and operators. Multi-photon cases can be implied through some statistical transformations.

An intrinsic problem in using photons as information carriers is that photons hardly interact with each other. This potentially causes a scalability problem for LOQC, since nonlinear operations are hard to implement, which can increase the complexity of operators and hence can increase the resources required

to realize a given computational function. One way to solve this problem is to bring nonlinear devices into the quantum network. For instance, the Kerr effect can be applied into LOQC to make a single-photon controlled-NOT and other operations.[10][11]

KLM protocol

It was believed that adding nonlinearity to the linear optical network was sufficient to realize efficient quantum computation.[12] However, to implement nonlinear optical effects is a difficult task. In 2000, Knill, Laflamme and Milburn proved that it is possible to create universal quantum computers solely with linear optical tools.[2] Their work has become known as the "KLM scheme" or "KLM protocol", which uses linear optical elements, single photon sources and photon detectors as resources to construct a quantum computation scheme involving only ancilla resources, quantum teleportations and error corrections. It uses another way of efficient quantum computation with linear optical systems, and promotes nonlinear operations solely with linear optical elements.[3]

At its root, the KLM scheme induces an effective interaction between photons by making projective measurements with photodetectors, which falls into the category of non-deterministic quantum computation. It is based on a non-linear sign shift between two qubits that uses two ancilla photons and post-selection.[13] It is also based on the demonstrations that the probability of success of the quantum gates can be made close to one by using entangled states prepared non-deterministically and quantum teleportation with single-qubit operations[14][15] Otherwise, without a high enough success rate of a single quantum gate unit, it may require an exponential amount of computing resources. Meanwhile, the KLM scheme is based on the fact that proper quantum coding can reduce the resources for obtaining accurately encoded qubits efficiently with respect to the accuracy achieved, and can make LOQC fault-tolerant for photon loss, detector inefficiency and phase decoherence. As a result, LOQC can be robustly implemented through the KLM scheme with a low enough resource requirement to suggest practical scalability, making it as promising a technology for QIP as other known implementations.

Boson sampling

The more limited boson sampling model was suggested and analyzed by Aaronson and Arkhipov in 2010.[16] It is not believed to be universal,[16] but can still solve problems that are believed to be beyond the ability of classical computers, such as the boson sampling problem. On Dec 3 2020 a team led by Chinese Physicist Pan Jianwei (潘建伟) and Lu Chaoyang (陆朝阳) from University of Science and Technology of China in Hefei, Anhui Province submitted their results to Science in which they solved a problem that is virtually unassailable by any classical computer; thereby proving Quantum supremacy of their photon-based quantum computer called Jiu Zhang Quantum Computer (九章量子计算机).[17] The boson sampling problem was solved in 200 seconds, they estimated that China's Sunway TaihuLight Supercomputer would take 2.5 billion years to solve - a quantum supremacy of around 10^14. Jiu Zhang was named in honor of China's oldest surviving mathematical text (Jiǔ zhāng suàn shù) The Nine Chapters on the Mathematical Art [18]

Ingredients

DiVincenzo's criteria for quantum computation and QIP[19][20] give that a universal system for QIP should satisfy at least the following requirements:

1. a scalable physical system with well characterized qubits,
2. the ability to initialize the state of the qubits to a simple fiducial state, such as $|000\cdots\rangle$,
3. long relevant decoherence times, much longer than the gate operation time,
4. a "universal" set of quantum gates (this requirement cannot be satisfied by a non-universal system),
5. a qubit-specific measurement capability;
   if the system is also aiming for quantum communication, it should also satisfy at least the following two requirements:
6. the ability to interconvert stationary and flying qubits, and
7. the ability to faithfully transmit flying qubits between specified location.

As a result of using photons and linear optical circuits, in general LOQC systems can easily satisfy conditions 3, 6 and 7.[3] The following sections mainly focus on the implementations of quantum information preparation, readout, manipulation, scalability and error corrections, in order to discuss the advantages and disadvantages of LOQC as a candidate for QIP

Qubits and modes

A qubit is one of the fundamental QIP units. A qubit state which can be represented by $\alpha|0\rangle + \beta|1\rangle$ is a superposition state which, if measured in the orthonormal basis $\{|0\rangle, |1\rangle\}$, has probability $|\alpha|^2$ of being in the $|0\rangle$ state and probability $|\beta|^2$ of being in the $|1\rangle$ state, where $|\alpha|^2 + |\beta|^2 = 1$ is the normalization condition. An optical mode is a distinguishable optical communication channel, which is usually labeled by subscripts of a quantum state. There are many ways to define distinguishable optical communication channels. For example, a set of modes could be different polarization of light which can be picked out with linear optical elements, various frequencies, or a combination of the two cases above.

In the KLM protocol, each of the photons is usually in one of two modes, and the modes are different between the photons (the possibility that a mode is occupied by more than one photon is zero). This is not the case only during implementations of controlled quantum gates such as CNOT. When the state of the system is as described, the photons can be distinguished, since they are in different modes, and therefore a qubit state can be represented using a single photon in two modes, vertical (V) and horizontal (H): for example, $|0\rangle \equiv |0,1\rangle_{VH}$ and $|1\rangle \equiv |1,0\rangle_{VH}$. It is common to refer to the states defined via occupation of modes as Fock states.

In boson sampling, photons are not distinguished, and therefore cannot directly represent the qubit state. Instead, we represent the qubit state of the entire quantum system by using the Fock states of M modes which are occupied by N indistinguishable single photons (this is a $\binom{M+N-1}{M}$-level quantum system).

State preparation

To prepare a desired multi-photon quantum state for LOQC, a single-photon state is first required. Therefore, non-linear optical elements, such as single-photon generators and some optical modules, will be employed. For example, optical parametric down-conversion can be used to conditionally generate the $|1\rangle \equiv |1,0\rangle_{VH}$ state in the vertical polarization channel at time t (subscripts are ignored for this single qubit case). By using a conditional single-photon source, the output state is guaranteed, although this may

require several attempts (depending on the success rate). A joint multi-qubit state can be prepared in a similar way. In general, an arbitrary quantum state can be generated for QIP with a proper set of photon sources.

Implementations of elementary quantum gates

To achieve universal quantum computing, LOQC should be capable of realizing a complete set of universal gates. This can be achieved in the KLM protocol but not in the boson sampling model.

Ignoring error correction and other issues, the basic principle in implementations of elementary quantum gates using only mirrors, beam splitters and phase shifters is that by using these linear optical elements, one can construct any arbitrary 1-qubit unitary operation; in other words, those linear optical elements support a complete set of operators on any single qubit.

The unitary matrix associated with a beam splitter $\mathbf{B}_{\theta,\phi}$ is:

$$U(\mathbf{B}_{\theta,\phi}) = \begin{bmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & \cos\theta \end{bmatrix},$$

where θ and ϕ are determined by the reflection amplitude r and the transmission amplitude t (relationship will be given later for a simpler case). For a symmetric beam splitter, which has a phase shift $\phi = \dfrac{\pi}{2}$ under the unitary transformation condition $|t|^2 + |r|^2 = 1$ and $t^*r + tr^* = 0$, one can show that

$$U(\mathbf{B}_{\theta,\phi=\frac{\pi}{2}}) = \begin{bmatrix} t & r \\ r & t \end{bmatrix} = \begin{bmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{bmatrix} = \cos\theta\hat{I} - i\sin\theta\hat{\sigma}_x = e^{-i\theta\hat{\sigma}_x},$$

which is a rotation of the single qubit state about the x-axis by $2\theta = 2\cos^{-1}(|t|)$ in the Bloch sphere.

A mirror is a special case where the reflecting rate is 1, so that the corresponding unitary operator is a rotation matrix given by

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

For most cases of mirrors used in QIP, the incident angle $\theta = 45^\circ$.

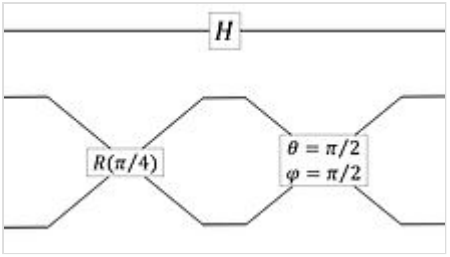
Similarly, a phase shifter operator $\mathbf{P}_\phi$ associates with a unitary operator described by $U(\mathbf{P}_\phi) = e^{i\phi}$, or, if written in a 2-mode format

$$U(\mathbf{P}_\phi) = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{bmatrix}(\text{global phase ignored}) = e^{i\frac{\phi}{2}\hat{\sigma}_z},$$

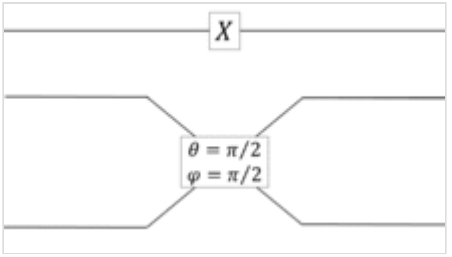
which is equivalent to a rotation of $-\phi$ about the z-axis.

Since any two $SU(2)$ rotations along orthogonal rotating axes can generate arbitrary rotations in the Bloch sphere, one can use a set of symmetric beam splitters and mirrors to realize an arbitrary $SU(2)$ operators for QIP. The figures below are examples of implementing a Hadamard gate and a Pauli-X-gate

(NOT gate) by using beam splitters (illustrated as rectangles connecting two sets of crossing lines with parameters θ and ϕ) and mirrors (illustrated as rectangles connecting two sets of crossing lines with parameter $R(\theta)$).



Implementation of a Hadamard gate with a beam splitter and a mirror. Quantum circuit is on the top part.



Implementation of a Pauli-X gate (NOT gate) with a beam splitter. Quantum circuit is on the top part.

In the above figures, a qubit is encoded using two mode channels (horizontal lines): $|0\rangle$ represents a photon in the top mode, and $|1\rangle$ represents a photon in the bottom mode.

Using integrated photonic circuits

In reality, assembling a whole bunch (possibly on the order of 10^4[21]) of beam splitters and phase shifters in an optical experimental table is challenging and unrealistic. To make LOQC functional, useful and compact, one solution is to miniaturize all linear optical elements, photon sources and photon detectors, and to integrate them onto a chip. If using a semiconductor platform, single photon sources and photon detectors can be easily integrated. To separate modes, there have been integrated arrayed waveguide grating (AWG) which are commonly used as optical (de)multiplexers in wavelength division multiplexed (WDM). In principle, beam splitters and other linear optical elements can also be miniaturized or replaced by equivalent nanophotonics elements. Some progress in these endeavors can be found in the literature, for example, Refs.[22][23][24] In 2013, the first integrated photonic circuit for quantum information processing has been demonstrated using photonic crystal waveguide to realize the interaction between guided field and atoms.[25]

Implementations comparison

Comparison of the KLM protocol and the boson sampling model

The advantage of the KLM protocol over the boson sampling model is that while the KLM protocol is a universal model, boson sampling is not believed to be universal. On the other hand, it seems that the scalability issues in boson sampling are more manageable than those in the KLM protocol.

In boson sampling only a single measurement is allowed, a measurement of all the modes at the end of the computation. The only scalability problem in this model arises from the requirement that all the photons arrive at the photon detectors within a short-enough time interval and with close-enough frequencies.[16]

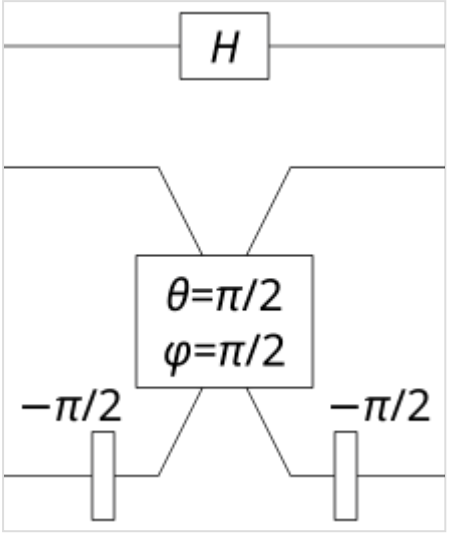
In the KLM protocol, there are non-deterministic quantum gates, which are essential for the model to be universal. These rely on gate teleportation, where multiple probabilistic gates are prepared offline and additional measurements are performed mid-circuit. Those two factors are the cause for additional scalability problems in the KLM protocol.

In the KLM protocol the desired initial state is one in which each of the photons is in one of two modes, and the possibility that a mode is occupied by more than one photon is zero. In boson sampling, however, the desired initial state is specific, requiring that the first N modes are each occupied by a single photon[16] (N is the number of photons and $M \geq N$ is the number of modes) and all the other states are empty.

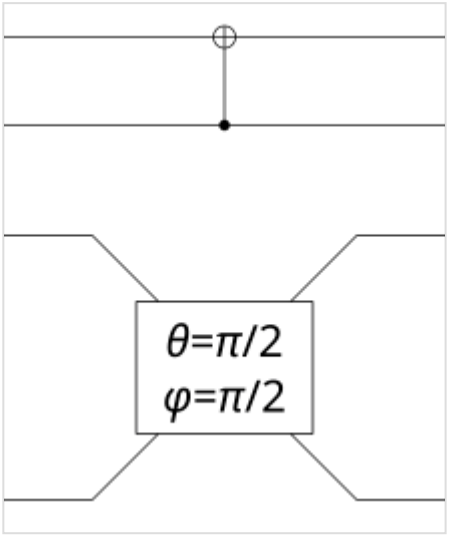
Earlier models

Another, earlier model which relies on the representation of several qubits by a single photon is based on the work of C. Adami and N. J. Cerf.[1] By using both the location and the polarization of photons, a single photon in this model can represent several qubits; however, as a result, CNOT-gate can only be implemented between the two qubits represented by the same photon.

The figures below are examples of making an equivalent Hadamard-gate and CNOT-gate using beam splitters (illustrated as rectangles connecting two sets of crossing lines with parameters θ and ϕ) and phase shifters (illustrated as rectangles on a line with parameter ϕ).



Implementation of Hadamard-gate on a "location" qubit with a beam splitter and phase shifters. Quantum circuit is on the top part.



Implementation of Controlled-NOT-gate with a beam splitter. Quantum circuit is on the top part.

In the optical realization of the CNOT gate, the polarization and location are the control and target qubit, respectively.

References

1. Adami, C.; Cerf, N. J. (1999). "Quantum Computation with Linear Optics". *Quantum Computing and Quantum Communications*. Lecture Notes in Computer Science. Vol. 1509.

Springer. pp. 391–401. arXiv:quant-ph/9806048 (https://arxiv.org/abs/quant-ph/9806048). doi:10.1007/3-540-49208-9_36 (https://doi.org/10.1007%2F3-540-49208-9_36). ISBN 978-3-540-65514-5. S2CID 5222656 (https://api.semanticscholar.org/CorpusID:5222656).

2. Knill, E.; Laflamme, R.; Milburn, G. J. (2001). "A scheme for efficient quantum computation with linear optics". *Nature*. **409** (6816): 46–52. Bibcode:2001Natur.409...46K (https://ui.adsabs.harvard.edu/abs/2001Natur.409...46K). doi:10.1038/35051009 (https://doi.org/10.1038%2F35051009). PMID 11343107 (https://pubmed.ncbi.nlm.nih.gov/11343107). S2CID 4362012 (https://api.semanticscholar.org/CorpusID:4362012).
3. Kok, P.; Munro, W. J.; Nemoto, K.; Ralph, T. C.; Dowling, J. P.; Milburn, G. J. (2007). "Linear optical quantum computing with photonic qubits". *Rev. Mod. Phys*. **79** (1): 135–174. arXiv:quant-ph/0512071 (https://arxiv.org/abs/quant-ph/0512071). Bibcode:2007RvMP...79..135K (https://ui.adsabs.harvard.edu/abs/2007RvMP...79..135K). doi:10.1103/RevModPhys.79.135 (https://doi.org/10.1103%2FRevModPhys.79.135). S2CID 119335959 (https://api.semanticscholar.org/CorpusID:119335959).
4. Lloyd, S.; Braunstein, S. L. (2003). "Quantum computation over continuous variables". *Physical Review Letters*. **82** (8): 9–17. arXiv:quant-ph/9810082 (https://arxiv.org/abs/quant-ph/9810082). Bibcode:1999PhRvL..82.1784L (https://ui.adsabs.harvard.edu/abs/1999PhRvL..82.1784L). doi:10.1103/PhysRevLett.82.1784 (https://doi.org/10.1103%2FPhysRevLett.82.1784). S2CID 119018466 (https://api.semanticscholar.org/CorpusID:119018466).
5. DiVincenzo, David P. (1995-02-01). "Two-bit gates are universal for quantum computation". *Physical Review A*. **51** (2): 1015–1022. arXiv:cond-mat/9407022 (https://arxiv.org/abs/cond-mat/9407022). Bibcode:1995PhRvA..51.1015D (https://ui.adsabs.harvard.edu/abs/1995PhRvA..51.1015D). doi:10.1103/PhysRevA.51.1015 (https://doi.org/10.1103%2FPhysRevA.51.1015). PMID 9911679 (https://pubmed.ncbi.nlm.nih.gov/9911679). S2CID 2317415 (https://api.semanticscholar.org/CorpusID:2317415).
6. Deutsch, David; Barenco, Adriano; Ekert, Artur (1995-06-08). "Universality in Quantum Computation". *Proceedings of the Royal Society of London A: Mathematical and Physical Sciences*. **449** (1937): 669–677. arXiv:quant-ph/9505018 (https://arxiv.org/abs/quant-ph/9505018). Bibcode:1995RSPSA.449..669D (https://ui.adsabs.harvard.edu/abs/1995RSPSA.449..669D). CiteSeerX 10.1.1.54.2646 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.54.2646). doi:10.1098/rspa.1995.0065 (https://doi.org/10.1098%2Frspa.1995.0065). ISSN 1471-2946 (https://search.worldcat.org/issn/1471-2946). S2CID 15088854 (https://api.semanticscholar.org/CorpusID:15088854).
7. Barenco, Adriano (1995-06-08). "A Universal Two-Bit Gate for Quantum Computation". *Proceedings of the Royal Society of London A: Mathematical and Physical Sciences*. **449** (1937): 679–683. arXiv:quant-ph/9505016 (https://arxiv.org/abs/quant-ph/9505016). Bibcode:1995RSPSA.449..679B (https://ui.adsabs.harvard.edu/abs/1995RSPSA.449..679B). doi:10.1098/rspa.1995.0066 (https://doi.org/10.1098%2Frspa.1995.0066). ISSN 1471-2946 (https://search.worldcat.org/issn/1471-2946). S2CID 119447556 (https://api.semanticscholar.org/CorpusID:119447556).
8. Lloyd, Seth (1995-07-10). "Almost Any Quantum Logic Gate is Universal". *Physical Review Letters*. **75** (2): 346–349. Bibcode:1995PhRvL..75..346L (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75..346L). doi:10.1103/PhysRevLett.75.346 (https://doi.org/10.1103%2FPhysRevLett.75.346). PMID 10059671 (https://pubmed.ncbi.nlm.nih.gov/10059671).
9. Reck, Michael; Zeilinger, Anton; Bernstein, Herbert J.; Bertani, Philip (1994-07-04). "Experimental realization of any discrete unitary operator" (https://zenodo.org/record/3452285). *Physical Review Letters*. **73** (1): 58–61. Bibcode:1994PhRvL..73...58R (https://ui.adsabs.harvard.edu/abs/1994PhRvL..73...58R). doi:10.1103/PhysRevLett.73.58 (https://doi.org/10.1103%2FPhysRevLett.73.58). PMID 10056719 (https://pubmed.ncbi.nlm.nih.gov/10056719).

10. Milburn, G. J. (1989-05-01). "Quantum optical Fredkin gate" (http://espace.library.uq.edu.au/view/UQ:247726/UQ247726.pdf) (PDF). *Physical Review Letters*. **62** (18): 2124–2127. Bibcode:1989PhRvL..62.2124M (https://ui.adsabs.harvard.edu/abs/1989PhRvL..62.2124M). doi:10.1103/PhysRevLett.62.2124 (https://doi.org/10.1103%2FPhysRevLett.62.2124). PMID 10039862 (https://pubmed.ncbi.nlm.nih.gov/10039862).
11. Hutchinson, G. D.; Milburn, G. J. (2004). "Nonlinear quantum optical computing via measurement". *Journal of Modern Optics*. **51** (8): 1211–1222. arXiv:quant-ph/0409198 (https://arxiv.org/abs/quant-ph/0409198). Bibcode:2004JMOp...51.1211H (https://ui.adsabs.harvard.edu/abs/2004JMOp...51.1211H). doi:10.1080/09500340408230417 (https://doi.org/10.1080%2F09500340408230417). ISSN 0950-0340 (https://search.worldcat.org/issn/0950-0340). S2CID 14246243 (https://api.semanticscholar.org/CorpusID:14246243).
12. Lloyd, Seth (1992-07-20). "Any nonlinear gate, with linear gates, suffices for computation" (https://zenodo.org/record/1258495). *Physics Letters A*. **167** (3): 255–260. Bibcode:1992PhLA..167..255L (https://ui.adsabs.harvard.edu/abs/1992PhLA..167..255L). doi:10.1016/0375-9601(92)90201-V (https://doi.org/10.1016%2F0375-9601%2892%29902001-V). ISSN 0375-9601 (https://search.worldcat.org/issn/0375-9601).
13. Adleman, Leonard M.; DeMarrais, Jonathan; Huang, Ming-Deh A. (1997). "Quantum Computability". *SIAM Journal on Computing*. **26** (5): 1524–1540. doi:10.1137/S0097539795293639 (https://doi.org/10.1137%2FS0097539795293639). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397).
14. Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K. (1993-03-29). "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels" (https://doi.org/10.1103%2FPhysRevLett.70.1895). *Physical Review Letters*. **70** (13): 1895–1899. Bibcode:1993PhRvL..70.1895B (https://ui.adsabs.harvard.edu/abs/1993PhRvL..70.1895B). doi:10.1103/PhysRevLett.70.1895 (https://doi.org/10.1103%2FPhysRevLett.70.1895). PMID 10053414 (https://pubmed.ncbi.nlm.nih.gov/10053414).
15. Gottesman, Daniel; Chuang, Isaac L. (1999-11-25). "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". *Nature*. **402** (6760): 390–393. arXiv:quant-ph/9908010 (https://arxiv.org/abs/quant-ph/9908010). Bibcode:1999Natur.402..390G (https://ui.adsabs.harvard.edu/abs/1999Natur.402..390G). doi:10.1038/46503 (https://doi.org/10.1038%2F46503). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). S2CID 119342550 (https://api.semanticscholar.org/CorpusID:119342550).
16. Aaronson, Scott; Arkhipov, Alex (2013). "The computational complexity of linear optics" (https://doi.org/10.4086%2Ftoc.2013.v009a004). *Theory of Computing*. **9**: 143–252. doi:10.4086/toc.2013.v009a004 (https://doi.org/10.4086%2Ftoc.2013.v009a004).
17. Ball, Philip (2020). "Physicists in China challenge Google's 'quantum advantage' " (https://www.nature.com/articles/d41586-020-03434-7). *Nature*. **588** (7838): 380. Bibcode:2020Natur.588..380B (https://ui.adsabs.harvard.edu/abs/2020Natur.588..380B). doi:10.1038/d41586-020-03434-7 (https://doi.org/10.1038%2Fd41586-020-03434-7). PMID 33273711 (https://pubmed.ncbi.nlm.nih.gov/33273711). S2CID 227282052 (https://api.semanticscholar.org/CorpusID:227282052).
18. "China claims quantum computing lead with Jiuzhang photon test, creating machine 'one trillion times faster' than next best supercomputer" (https://www.scmp.com/news/china/science/article/3112649/china-claims-quantum-computing-lead-jiuzhang-photon-test.). *SCMP*.
19. DiVincenzo, D.; Loss, D. (1998). "Quantum information is physical". *Superlattices and Microstructures*. **23** (3–4): 419–432. arXiv:cond-mat/9710259 (https://arxiv.org/abs/cond-mat/9710259). Bibcode:1998SuMi...23..419D (https://ui.adsabs.harvard.edu/abs/1998SuMi...23..419D). doi:10.1006/spmi.1997.0520 (https://doi.org/10.1006%2Fspmi.1997.0520). S2CID 6877353 (https://api.semanticscholar.org/CorpusID:6877353).

20. Divincenzo, D. P. (2000). "The Physical Implementation of Quantum Computation". *Fortschritte der Physik*. **48** (9–11): 771–783. arXiv:quant-ph/0002077 (https://arxiv.org/abs/quant-ph/0002077). Bibcode:2000ForPh..48..771D (https://ui.adsabs.harvard.edu/abs/2000ForPh..48..771D). doi:10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E (https://doi.org/10.1002%2F1521-3978%28200009%2948%3A9%2F11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E). S2CID 15439711 (https://api.semanticscholar.org/CorpusID:15439711).
21. Hayes, A. J. F.; Gilchrist, A.; Myers, C. R.; Ralph, T. C. (2004-12-01). "Utilizing encoding in scalable linear optics quantum computing". *Journal of Optics B: Quantum and Semiclassical Optics*. **6** (12): 533–541. arXiv:quant-ph/0408098 (https://arxiv.org/abs/quant-ph/0408098). Bibcode:2004JOptB...6..533H (https://ui.adsabs.harvard.edu/abs/2004JOptB...6..533H). doi:10.1088/1464-4266/6/12/008 (https://doi.org/10.1088%2F1464-4266%2F6%2F12%2F008). ISSN 1464-4266 (https://search.worldcat.org/issn/1464-4266). S2CID 119465216 (https://api.semanticscholar.org/CorpusID:119465216).
22. Gevaux, D (2008). "Optical quantum circuits: To the quantum level" (https://doi.org/10.1038%2Fnphoton.2008.92). *Nature Photonics*. **2** (6): 337. Bibcode:2008NaPho...2..337G (https://ui.adsabs.harvard.edu/abs/2008NaPho...2..337G). doi:10.1038/nphoton.2008.92 (https://doi.org/10.1038%2Fnphoton.2008.92).
23. Politi, A.; Cryan, M. J.; Rarity, J. G.; Yu, S.; O'Brien, J. L. (2008). "Silica-on-silicon waveguide quantum circuits". *Science*. **320** (5876): 646–649. arXiv:0802.0136 (https://arxiv.org/abs/0802.0136). Bibcode:2008Sci...320..646P (https://ui.adsabs.harvard.edu/abs/2008Sci...320..646P). doi:10.1126/science.1155441 (https://doi.org/10.1126%2Fscience.1155441). PMID 18369104 (https://pubmed.ncbi.nlm.nih.gov/18369104). S2CID 3234732 (https://api.semanticscholar.org/CorpusID:3234732).
24. Thompson, M. G.; Politi, A.; Matthews, J. C.; O'Brien, J. L. (2011). "Integrated waveguide circuits for optical quantum computing". *IET Circuits, Devices & Systems*. **5** (2): 94–102. doi:10.1049/iet-cds.2010.0108 (https://doi.org/10.1049%2Fiet-cds.2010.0108).
25. Goban, A.; Hung, C. -L.; Yu, S. -P.; Hood, J. D.; Muniz, J. A.; Lee, J. H.; Martin, M. J.; McClung, A. C.; Choi, K. S.; Chang, D. E.; Painter, O.; Kimble, H. J. (2013). "Atom-Light Interactions in Photonic Crystals". *Nature Communications*. **5**: 3808. arXiv:1312.3446 (https://arxiv.org/abs/1312.3446). Bibcode:2014NatCo...5.3808G (https://ui.adsabs.harvard.edu/abs/2014NatCo...5.3808G). doi:10.1038/ncomms4808 (https://doi.org/10.1038%2Fncomms4808). PMID 24806520 (https://pubmed.ncbi.nlm.nih.gov/24806520). S2CID 337901 (https://api.semanticscholar.org/CorpusID:337901).

External links

- "Optical chip allows for reprogramming quantum computer in seconds" (http://www.kurzweilai.net/optical-chip-allows-for-reprogramming-quantum-computer-in-seconds). kurzweilai.net. August 14, 2015.
- *The Mathematics of Quantum Computers* | *Infinite Series* (https://www.youtube.com/watch?v=IrbJYsep45E), retrieved 2019-11-23

Retrieved from "https://en.wikipedia.org/w/index.php?title=Linear_optical_quantum_computing&oldid=1191259241"

WIKIPEDIA
The Free Encyclopedia

KLM protocol

The **KLM scheme** or **KLM protocol** is an implementation of linear optical quantum computing (LOQC) developed in 2000 by Emanuel Knill, Raymond Laflamme and Gerard J. Milburn. This protocol allows for the creation of universal quantum computers using solely linear optical tools.[1] The KLM protocol uses linear optical elements, single-photon sources and photon detectors as resources to construct a quantum computation scheme involving only ancilla resources, quantum teleportations and error corrections.

Overview

The KLM scheme induces an effective interaction between photons by making projective measurements with photodetectors, which falls into the category of non-deterministic quantum computation. It is based on a non-linear sign shift between two qubits that uses two ancilla photons and post-selection.[2] It is also based on the demonstrations that the probability of success of the quantum gates can be made close to one by using entangled states prepared non-deterministically and quantum teleportation with single-qubit operations.[3][4] Without a high enough success rate of a single quantum gate unit, it may require an exponential amount of computing resources. The KLM scheme is based on the fact that proper quantum coding can reduce the resources for obtaining accurately encoded qubits efficiently with respect to the accuracy achieved, and can make LOQC fault-tolerant for photon loss, detector inefficiency and phase decoherence. LOQC can be robustly implemented through the KLM scheme with a low enough resource requirement to suggest practical scalability, making it as promising a technology for quantum information processing as other known implementations.

Elements of LOQC in the KLM scheme

Qubits and modes

To avoid losing generality, the discussion below does not limit itself to a particular instance of mode representation. A state written as $|0,1\rangle_{VH}$ means a state with zero photons in mode V (could be the "vertical" polarization channel) and one photon in the mode H (could be the "horizontal" polarization channel).

In the KLM protocol, each of the photons is usually in one of two modes, and the modes are different between the photons (the possibility that a mode is occupied by more than one photon is zero). This is not the case only during implementations of controlled quantum gates such as CNOT. When the state of the system is as described, the photons can be distinguished, since they are in different modes, and therefore a qubit state can be represented using a single photon in two modes, vertical (V) and horizontal (H): for example, $|0\rangle \equiv |0,1\rangle_{VH}$ and $|1\rangle \equiv |1,0\rangle_{VH}$. It is common to refer to the states defined via occupation of modes as Fock states.

Such notations are useful in quantum computing, quantum communication and quantum cryptography. For example, it is very easy to consider a loss of a single photon using these notations, simply by adding the vacuum state $|0,0\rangle_{VH}$ containing zero photons in those two modes. As another example, when having two photons in two separated modes (e.g. two time bins or two arms of an interferometer), it is easy to describe an entangled state of the two photons. The singlet state (two linked photons with overall spin quantum number $s = 0$) can be described as follows: if $|1,0\rangle_{VH}^{a}, |0,1\rangle_{VH}^{a}$ and $|1,0\rangle_{VH}^{b}, |0,1\rangle_{VH}^{b}$ describe the basis states of the two separated modes, then the singlet state is $(|1,0\rangle_{VH}^{a}|0,1\rangle_{VH}^{b} - |0,1\rangle_{VH}^{a}|1,0\rangle_{VH}^{b})/\sqrt{2}$.

State measurement/readout

In the KLM protocol, a quantum state can be read out or measured using photon detectors along selected modes. If a photodetector detects a photon signal in a given mode, it means the corresponding mode state is a 1-photon state before measuring. As discussed in KLM's proposal,[1] photon loss and detection efficiency dramatically influence the reliability of the measurement results. The corresponding failure issue and error correction methods will be described later.

A left-pointed triangle will be used in circuit diagrams to represent the state readout operator in this article.[1]

Implementations of elementary quantum gates

Ignoring error correction and other issues, the basic principle in implementations of elementary quantum gates using only mirrors, beam splitters and phase shifters is that by using these linear optical elements, one can construct any arbitrary 1-qubit unitary operation; in other words, those linear optical elements support a complete set of operators on any single qubit.

The unitary matrix associated with a beam splitter $\mathbf{B}_{\theta,\phi}$ is:

$$U(\mathbf{B}_{\theta,\phi}) = \begin{bmatrix} \cos\theta & -e^{i\phi}\sin\theta \\ e^{-i\phi}\sin\theta & \cos\theta \end{bmatrix},$$

where θ and ϕ are determined by the reflection amplitude r and the transmission amplitude t (relationship will be given later for a simpler case). For a symmetric beam splitter, which has a phase shift $\phi = \dfrac{\pi}{2}$ under the unitary transformation condition $|t|^2 + |r|^2 = 1$ and $t^*r + tr^* = 0$, one can show that

$$U(\mathbf{B}_{\theta,\phi=\frac{\pi}{2}}) = \begin{bmatrix} t & r \\ r & t \end{bmatrix} = \begin{bmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{bmatrix} = \cos\theta\hat{I} - i\sin\theta\hat{\sigma}_x = e^{-i\theta\hat{\sigma}_x},$$

which is a rotation of the single qubit state about the x-axis by $2\theta = 2\cos^{-1}(|t|)$ in the Bloch sphere.

A mirror is a special case where the reflecting rate is 1, so that the corresponding unitary operator is a rotation matrix given by

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

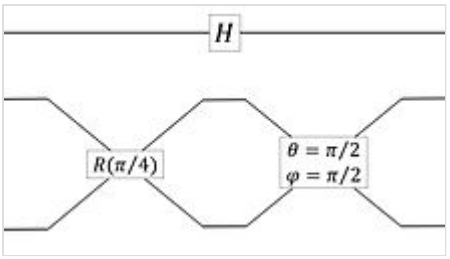
For most cases of beam splitters used in QIP, the incident angle $\theta = 45^\circ$.

Similarly, a phase shifter operator $\mathbf{P}_\phi$ associates with a unitary operator described by $U(\mathbf{P}_\phi) = e^{i\phi}$, or, if written in a 2-mode format

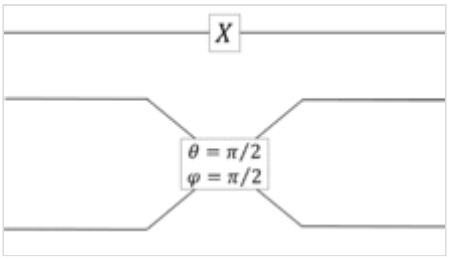
$$U(\mathbf{P}_\phi) = \begin{bmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{bmatrix} (\text{global phase ignored}) = e^{i\frac{\phi}{2}\hat{\sigma}_z},$$

which is equivalent to a rotation of $-\phi$ about the z-axis.

Since any two $SU(2)$ rotations along orthogonal rotating axes can generate arbitrary rotations in the Bloch sphere, one can use a set of symmetric beam splitters and mirrors to realize an arbitrary $SU(2)$ operators for QIP. The figures below are examples of implementing a Hadamard gate and a Pauli-X-gate (NOT gate) by using beam splitters (illustrated as rectangles connecting two sets of crossing lines with parameters θ and ϕ) and mirrors (illustrated as rectangles connecting two sets of crossing lines with parameter $R(\theta)$).



Implementation of a Hadamard gate with a beam splitter and a mirror. Quantum circuit is on the top part.



Implementation of a Pauli-X gate (NOT gate) with a beam splitter. Quantum circuit is on the top part.

In the above figures, a qubit is encoded using two mode channels (horizontal lines): $|0\rangle$ represents a photon in the top mode, and $|1\rangle$ represents a photon in the bottom mode.

In the KLM scheme, qubit manipulations are realized via a series of non-deterministic operations with increasing probability of success. The first improvement to this implementation that will be discussed is the nondeterministic conditional sign flip gate.

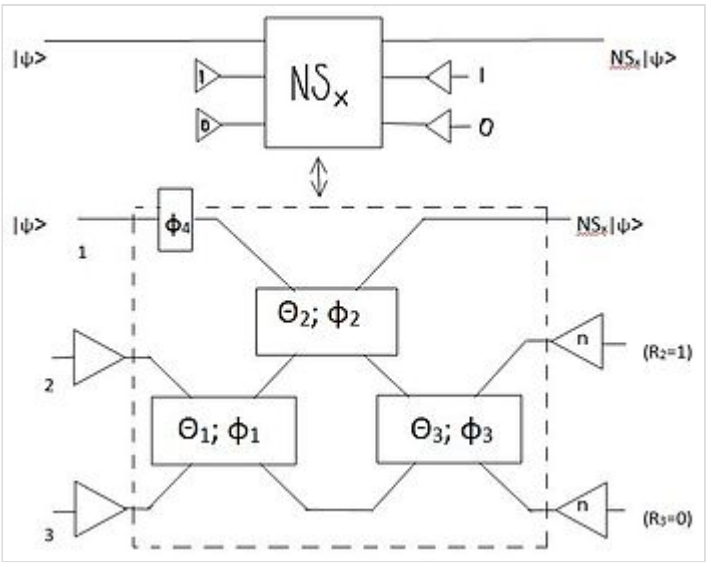
Implementation of nondeterministic conditional sign flip gate

An important element of the KLM scheme is the conditional sign flip or nonlinear sign flip gate (**NS-gate**) as shown in the figure below on the right. It gives a nonlinear phase shift on one mode conditioned on two ancilla modes.

In the picture on the right, the labels on the left of the bottom box indicate the modes. The output is accepted only if there is one photon in mode 2 and zero photons in mode 3 detected, where the ancilla modes 2 and 3 are prepared as the $|1,0\rangle_{2,3}$ state. The subscript x is the phase shift of the output, and is determined by the parameters of inner optical elements chosen.[1] For $x = -1$ case, the following parameters are used: $\theta_1 = 22.5^\circ$, $\phi_1 = 0^\circ$, $\theta_2 = 65.5302^\circ$, $\phi_2 = 0^\circ$, $\theta_3 = -22.5^\circ$, $\phi_3 = 0^\circ$, and $\phi_4 = 180^\circ$. For the $x = e^{i\pi/2}$ case, the parameters can be chosen as $\theta_1 = 36.53^\circ$, $\phi_1 = 88.24^\circ$, $\theta_2 = 62.25^\circ$, $\phi_2 = -66.53^\circ$, $\theta_3 = -36.53^\circ$, $\phi_3 = -11.25^\circ$, and $\phi_4 = 102.24^\circ$. Similarly, by

changing the parameters of beam splitters and phase shifters, or by combining multiple NS gates, one can create various quantum gates. By sharing two ancilla modes, Knill invented the following controlled-Z gate (see the figure on the right) with success rate of 2/27.[5]

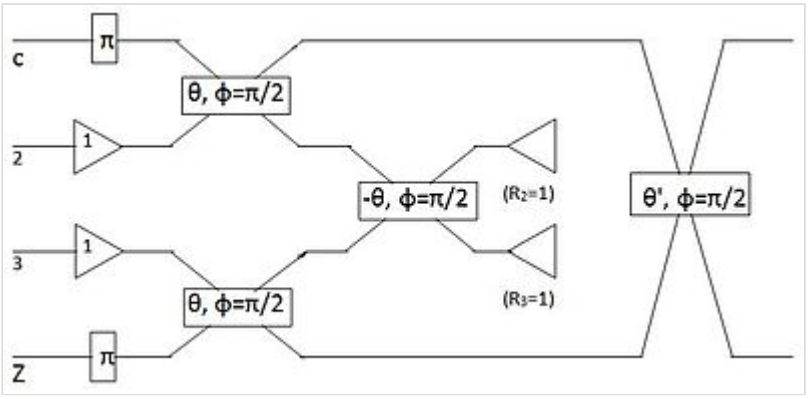
The advantage of using NS gates is that the output can be guaranteed conditionally processed with some success rate which can be improved to nearly 1. Using the configuration as shown in the figure above on the right, the success rate of an $x = -1$ NS gate is $1/4$. To further improve successful rate and solve the scalability problem, one needs to use gate teleportation, described next.



Linear optics implementation of NS-gate. The elements framed in the box with dashed border is the linear optics implementation with three beam splitters and one phase shifter (see text for parameters). Modes 2 and 3 are ancilla modes.

Gates teleportation and near-deterministic gates

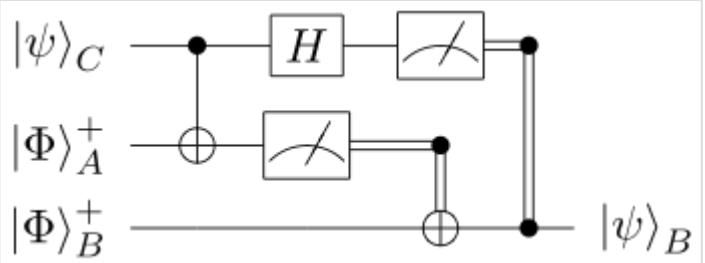
Given the use of non-deterministic quantum gates for KLM, there may be only a very small probability p^N that a circuit with N gates with a single-gate success possibility of p will work perfectly by running the circuit once. Therefore, the operations must on average be repeated on the order of p^{-N} times or p^{-N} such systems must be run in parallel. Either way, the required time or circuit resources scale exponentially. In 1999, Gottesman and Chuang pointed out that one can prepare the probabilistic gates offline from the quantum circuit by using quantum teleportation.[4] The basic idea is that each probabilistic gate is prepared offline, and the successful event signal is teleported back to the quantum circuit. An illustration of quantum teleportation is given in the figure on the right. As can be seen, the quantum state in mode 1 is teleported to mode 3 through a Bell measurement and an entangled resource Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, where the state 1 may be regarded as prepared offline.



Linear optics implementation of Controlled-Z Gate with ancilla modes labelled as 2 and 3. $\theta = 54.74°$ and $\theta' = 17.63°$.

The resource Bell state $|\Phi^+\rangle$ can be generated from the state $|10\rangle$ by use of a mirror with parameter $\theta = \frac{\pi}{4}$.

By using teleportation, many probabilistic gates may be prepared in parallel with n-photon entangled states, sending a control signal to the output mode. Through using n probabilistic gates in parallel offline, a success rate of $\frac{n^2}{(n+1)^2}$ can be obtained, which is close to 1 as n becomes large. The number of gates needed to realize a certain accuracy scales polynomially rather than exponentially. In this sense, the KLM protocol is resource-efficient. One experiment using the KLM originally proposed controlled-NOT gate with four-photon input was demonstrated in 2011,[6] and gave an average fidelity of $F = 0.82 \pm 0.01$.



Quantum circuit representation of quantum teleportation.

Error detection and correction

As discussed above, the success probability of teleportation gates can be made arbitrarily close to 1 by preparing larger entangled states. However, the asymptotic approach to the probability of 1 is quite slow with respect to the photon number n. A more efficient approach is to encode against gate failure (error) based on the well-defined failure mode of the teleporters. In the KLM protocol, the teleporter's failure can be diagnosed if zero or $n+1$ photons are detected. If the computing device can be encoded against accidental measurements of some certain number of photons, then it will be possible to correct gate failures and the probability of eventually successfully applying the gate will increase.

Many experimental trials using this idea have been carried out (see, for example, Refs[7][8][9]). However, a large number of operations are still needed to achieve a success probability very close to 1. In order to promote the KLM protocol as a viable technology, more efficient quantum gates are needed. This is the subject of the next part.

Improvements

This section discusses the improvements of the KLM protocol that have been studied after the initial proposal.

There are many ways to improve the KLM protocol for LOQC and to make LOQC more promising. Below are some proposals from the review article Ref.[10] and other subsequent articles:

- Using cluster states in optical quantum computing.
- Circuit-based optical quantum computing revisited.
- Using one-step deterministic multipartite entanglement purification with linear optics to generate entangled photon states.[11]

There are several protocols for using cluster states to improve the KLM protocol, the computation model with those protocols is an LOQC implementation of the one-way quantum computer:

- The Yoran-Reznik protocol - this protocol makes use of cluster-chains in order to increase the success probability of teleportation.
- The Nielsen protocol - this protocol improves the Yoran-Reznik protocol by first using teleportation to add qubits to cluster-chains and then uses the enlarged cluster chains to

further increase the success probability of teleportation.
- The Browne-Rudolph protocol - this protocol improves the Nielsen protocol by using teleportation not only to add qubits to cluster-chains but also to fuse them .

See also

- Boson sampling

References

1. Knill, E.; Laflamme, R.; Milburn, G. J. (2001). "A scheme for efficient quantum computation with linear optics". *Nature*. **409** (6816). Nature Publishing Group: 46–52. Bibcode:2001Natur.409...46K (https://ui.adsabs.harvard.edu/abs/2001Natur.409...46K). doi:10.1038/35051009 (https://doi.org/10.1038%2F35051009). PMID 11343107 (https://pubmed.ncbi.nlm.nih.gov/11343107). S2CID 4362012 (https://api.semanticscholar.org/CorpusID:4362012).
2. Adleman, Leonard M.; DeMarrais, Jonathan; Huang, Ming-Deh A. (1997). "Quantum Computability". *SIAM Journal on Computing*. **26** (5): 1524–1540. doi:10.1137/S0097539795293639 (https://doi.org/10.1137%2FS0097539795293639). ISSN 0097-5397 (https://search.worldcat.org/issn/0097-5397).
3. Bennett, Charles H.; Brassard, Gilles; Crépeau, Claude; Jozsa, Richard; Peres, Asher; Wootters, William K. (1993-03-29). "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels" (https://doi.org/10.1103%2FPhysRevLett.70.1895). *Physical Review Letters*. **70** (13): 1895–1899. Bibcode:1993PhRvL..70.1895B (https://ui.adsabs.harvard.edu/abs/1993PhRvL..70.1895B). doi:10.1103/PhysRevLett.70.1895 (https://doi.org/10.1103%2FPhysRevLett.70.1895). PMID 10053414 (https://pubmed.ncbi.nlm.nih.gov/10053414).
4. Gottesman, Daniel; Chuang, Isaac L. (1999-11-25). "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". *Nature*. **402** (6760): 390–393. arXiv:quant-ph/9908010 (https://arxiv.org/abs/quant-ph/9908010). Bibcode:1999Natur.402..390G (https://ui.adsabs.harvard.edu/abs/1999Natur.402..390G). doi:10.1038/46503 (https://doi.org/10.1038%2F46503). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). S2CID 4411647 (https://api.semanticscholar.org/CorpusID:4411647).
5. Knill, E. (2002-11-14). "Quantum gates using linear optics and postselection". *Physical Review A*. **66** (5): 052306. arXiv:quant-ph/0110144 (https://arxiv.org/abs/quant-ph/0110144). Bibcode:2002PhRvA..66e2306K (https://ui.adsabs.harvard.edu/abs/2002PhRvA..66e2306K). doi:10.1103/PhysRevA.66.052306 (https://doi.org/10.1103%2FPhysRevA.66.052306). S2CID 119529530 (https://api.semanticscholar.org/CorpusID:119529530).
6. Okamoto, Ryo; O'Brien, Jeremy L.; Hofmann, Holger F.; Takeuchi, Shigeki (2011-06-21). "Realization of a Knill-Laflamme-Milburn controlled-NOT photonic quantum circuit combining effective optical nonlinearities" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3121828). *Proceedings of the National Academy of Sciences*. **108** (25): 10067–10071. arXiv:1006.4743 (https://arxiv.org/abs/1006.4743). Bibcode:2011PNAS..10810067O (https://ui.adsabs.harvard.edu/abs/2011PNAS..10810067O). doi:10.1073/pnas.1018839108 (https://doi.org/10.1073%2Fpnas.1018839108). ISSN 0027-8424 (https://search.worldcat.org/issn/0027-8424). PMC 3121828 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3121828). PMID 21646543 (https://pubmed.ncbi.nlm.nih.gov/21646543).

7. O'Brien, J. L.; Pryde, G. J.; White, A. G.; Ralph, T. C. (2005-06-09). "High-fidelity Z-measurement error encoding of optical qubits". *Physical Review A*. **71** (6): 060303. arXiv:quant-ph/0408064 (https://arxiv.org/abs/quant-ph/0408064). Bibcode:2005PhRvA..71f0303O (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71f0303O). doi:10.1103/PhysRevA.71.060303 (https://doi.org/10.1103%2FPhysRevA.71.060303). S2CID 21661867 (https://api.semanticscholar.org/CorpusID:21661867).
8. Hayes, A. J. F.; Gilchrist, A.; Myers, C. R.; Ralph, T. C. (2004-12-01). "Utilizing encoding in scalable linear optics quantum computing". *Journal of Optics B: Quantum and Semiclassical Optics*. **6** (12). IOP Publishing: 533–541. arXiv:quant-ph/0408098 (https://arxiv.org/abs/quant-ph/0408098). Bibcode:2004JOptB...6..533H (https://ui.adsabs.harvard.edu/abs/2004JOptB...6..533H). doi:10.1088/1464-4266/6/12/008 (https://doi.org/10.1088%2F1464-4266%2F6%2F12%2F008). ISSN 1464-4266 (https://search.worldcat.org/issn/1464-4266). S2CID 119465216 (https://api.semanticscholar.org/CorpusID:119465216).
9. Pittman, T. B.; Jacobs, B. C.; Franson, J. D. (2005-05-31). "Demonstration of quantum error correction using linear optics". *Physical Review A*. **71** (5): 052332. arXiv:quant-ph/0502042 (https://arxiv.org/abs/quant-ph/0502042). Bibcode:2005PhRvA..71e2332P (https://ui.adsabs.harvard.edu/abs/2005PhRvA..71e2332P). doi:10.1103/PhysRevA.71.052332 (https://doi.org/10.1103%2FPhysRevA.71.052332). S2CID 11679660 (https://api.semanticscholar.org/CorpusID:11679660).
10. Kok, P.; Munro, W. J.; Nemoto, K.; Ralph, T. C.; Dowling, J. P.; Milburn, G. J. (2007). "Linear optical quantum computing with photonic qubits". *Rev. Mod. Phys*. **79** (1). American Physical Society: 135–174. arXiv:quant-ph/0512071 (https://arxiv.org/abs/quant-ph/0512071). Bibcode:2007RvMP...79..135K (https://ui.adsabs.harvard.edu/abs/2007RvMP...79..135K). doi:10.1103/RevModPhys.79.135 (https://doi.org/10.1103%2FRevModPhys.79.135). S2CID 119335959 (https://api.semanticscholar.org/CorpusID:119335959).
11. Sheng, Y.-B.; Long, G. L.; Deng, F.-G. (2012). "One-step deterministic multipartite entanglement purification with linear optics" (https://zenodo.org/record/948907). *Physics Letters A*. **2012** (376): 314–319. Bibcode:2012PhLA..376..314S (https://ui.adsabs.harvard.edu/abs/2012PhLA..376..314S). doi:10.1016/j.physleta.2011.09.056 (https://doi.org/10.1016%2Fj.physleta.2011.09.056). Archived (https://web.archive.org/web/20210129165427/https://zenodo.org/record/948907) from the original on 2021-01-29. Retrieved 2023-08-13.

Retrieved from "https://en.wikipedia.org/w/index.php?title=KLM_protocol&oldid=1226989465"

WIKIPEDIA
The Free Encyclopedia

Ultracold atom

In condensed matter physics, an **ultracold atom** is an atom with a temperature near absolute zero. At such temperatures, an atom's quantum-mechanical properties become important.

To reach such low temperatures, a combination of several techniques typically has to be used.[1] First, atoms are trapped and pre-cooled via laser cooling in a magneto-optical trap. To reach the lowest possible temperature, further cooling is performed using evaporative cooling in a magnetic or optical trap. Several Nobel prizes in physics are related to the development of the techniques to manipulate quantum properties of individual atoms (e.g. 1989, 1996, 1997, 2001, 2005, 2012, 2018).

Experiments with ultracold atoms study a variety of phenomena, including quantum phase transitions, Bose–Einstein condensation (BEC), bosonic superfluidity, quantum magnetism, many-body spin dynamics, Efimov states, Bardeen–Cooper–Schrieffer (BCS) superfluidity and the BEC–BCS crossover.[2] Some of these research directions utilize ultracold atom systems as quantum simulators to study the physics of other systems, including the unitary Fermi gas and the Ising and Hubbard models.[3] Ultracold atoms could also be used for realization of quantum computers.[4][5]

History

Samples of ultracold atoms are typically prepared through the interactions of a dilute gas with a laser field. Evidence for radiation pressure, force due to light on atoms, was demonstrated independently by Lebedev, and Nichols and Hull in 1901. In 1933, Otto Frisch demonstrated the deflection of individual sodium particles by light generated from a sodium lamp.

The invention of the laser spurred the development of additional techniques to manipulate atoms with light. Using laser light to cool atoms was first proposed in 1975 by taking advantage of the Doppler effect to make the radiation force on an atom dependent on its velocity, a technique known as Doppler cooling. Similar ideas were also proposed to cool samples of trapped ions. Applying Doppler cooling in three dimensions will slow atoms to velocities that are typically a few cm/s and produce what is known as an optical molasses.[6]

Typically, the source of neutral atoms for these experiments were thermal ovens which produced atoms at temperatures of a few hundred kelvins. The atoms from these oven sources are moving at hundred of meters per second. One of the major technical challenges in Doppler cooling was increasing the amount of time an atom can interact with the laser light. This challenge was overcome by the introduction of a Zeeman Slower. A Zeeman Slower uses a spatially varying magnetic field to maintain the relative energy spacing of the atomic transitions involved in Doppler cooling. This increases the amount of time the atom spends interacting with the laser light. Experiments can also use metal dispensers, which are pure metal (typically alkali metals) rods that can emit when heated up (the vapor pressure is higher) with electrical current.

The development of the first magneto-optical trap (MOT) by Raab et al. in 1987 was an important step towards the creation of samples of ultracold atoms. Typical temperatures achieved with a MOT are tens to hundreds of microkelvins. In essence, a magneto optical trap confines atoms in space by applying a magnetic field so that lasers not only provide a velocity dependent force but also a spatially varying force. The 1997 Nobel prize[6] in physics was awarded for development of methods to cool and trap atoms with laser light and was shared by Steven Chu, Claude Cohen-Tannoudji and William D. Phillips.

Evaporative cooling was used in experimental efforts to reach lower temperatures in an effort to discover a new state of matter predicted by Satyendra Nath Bose and Albert Einstein known as a Bose–Einstein condensate (BEC). In evaporative cooling, the hottest atoms in a sample are allowed to escape which reduces the average temperature of the sample. The Nobel Prize in 2001[1] was awarded to Eric A. Cornell, Wolfgang Ketterle and Carl E. Wieman for the achievement of Bose–Einstein condensate in dilute gases of alkali atoms, and for early fundamental studies of the properties of the condensates.

In recent years a variety of sub-Doppler cooling techniques, including polarization gradient cooling, gray molasses cooling, and Raman sideband cooling, have enabled the cooling and trapping of single atoms in optical tweezers.[7][8][9] Experimental platforms leveraging ultracold neutral atoms in optical tweezers and optical lattices have become an increasingly popular setting for studying quantum computing, quantum simulation, and precision metrology. Atoms with closed cycling transitions, capable of scattering many photons with a low probability of decay into other states, are common choices of species for ultracold neutral atom experiments. The lowest-energy fine structure transitions in alkali atoms enable fluorescence imaging, while a combination of hyperfine and Zeeman sublevels can be used for implementing sub-Doppler cooling. Alkaline earth atoms have also gained popularity owing to narrow-linewidth cooling transitions and ultra-narrow optical clock transitions.

Applications

Ultracold atoms have a variety of applications owing to their unique quantum properties and the great experimental control available in such systems. For instance, ultracold atoms have been proposed as a platform for quantum computation and quantum simulation,[10] accompanied by very active experimental research to achieve these goals.

Quantum simulation is of great interest in the context of condensed matter physics, where it may provide valuable insights into the properties of interacting quantum systems. The ultracold atoms are used to implement an analogue of the condensed matter system of interest, which can then be explored using the tools available in the particular implementation. Since these tools may differ greatly from those available in the actual condensed matter system, one can thus experimentally probe otherwise inaccessible quantities. Furthermore, ultracold atoms may even allow to create exotic states of matter, which cannot otherwise be observed in nature.

All atoms are identical, making ensembles of atoms ideal for universal timekeeping. In 1967, the SI definition of the second was changed to reference a hyperfine transition frequency in Cesium atoms. Atomic clocks based on alkaline earth atoms or alkaline earth like ions (such as Al^+) have now been developed making use of narrow-line optical transitions. To achieve high numbers of non-interacting atoms, which assists in the precision of these clocks, neutral atoms can be trapped in optical lattices. On the other hand, ion traps permit long interrogation times.

Ultracold atoms are also used in experiments for precision measurements enabled by the low thermal noise and, in some cases, by exploiting quantum mechanics to exceed the standard quantum limit. In addition to potential technical applications, such precision measurements may serve as tests of our current understanding of physics.

See also

- Bose–Einstein condensate
- Cold Atom Laboratory
- Quantum simulator

References

1. "The 2001 Nobel Prize in Physics - Popular Information" (https://www.nobelprize.org/nobel_prizes/physics/laureates/2001/popular.html). *www.nobelprize.org*. Retrieved 2016-01-27.
2. Madison, K. W.; Wang, Y. Q.; Rey, A. M.; et al., eds. (2013). *Annual Review of Cold Atoms and Molecules*. Vol. 1. World Scientific. doi:10.1142/8632 (https://doi.org/10.1142%2F8632). ISBN 978-981-4440-39-4.
3. Bloch, Immanuel; Dalibard, Jean; Nascimbène, Sylvain (2012). "Quantum simulations with ultracold quantum gases". *Nature Physics*. **8** (4): 267–276. Bibcode:2012NatPh...8..267B (https://ui.adsabs.harvard.edu/abs/2012NatPh...8..267B). doi:10.1038/nphys2259 (https://doi.org/10.1038%2Fnphys2259). S2CID 17023076 (https://api.semanticscholar.org/CorpusID:17023076).
4. Nemirovsky, Jonathan; Sagi, Yoav (2021), "Fast universal two-qubit gate for neutral fermionic atoms in optical tweezers", *Physical Review Research*, **3** (1): 013113, arXiv:2008.09819 (https://arxiv.org/abs/2008.09819), Bibcode:2021PhRvR...3a3113N (https://ui.adsabs.harvard.edu/abs/2021PhRvR...3a3113N), doi:10.1103/PhysRevResearch.3.013113 (https://doi.org/10.1103%2FPhysRevResearch.3.013113)
5. Bluvstein, Dolev; Evered, Simon J.; Geim, Alexandra A.; Li, Sophie H.; Zhou, Hengyun; Manovitz, Tom; Ebadi, Sepehr; Cain, Madelyn; Kalinowski, Marcin; Hangleiter, Dominik; Bonilla Ataides, J. Pablo; Maskara, Nishad; Cong, Iris; Gao, Xun; Sales Rodriguez, Pedro. "Logical quantum processor based on reconfigurable atom arrays" (https://www.nature.com/articles/s41586-023-06927-3). *Nature*. **626** (7997): 58–65. arXiv:2312.03982 (https://arxiv.org/abs/2312.03982). doi:10.1038/s41586-023-06927-3 (https://doi.org/10.1038%2Fs41586-023-06927-3). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687).
6. "Press Release: The 1997 Nobel Prize in Physics" (https://www.nobelprize.org/nobel_prizes/physics/laureates/1997/press.html). *www.nobelprize.org*. Retrieved 2016-01-27.
7. Dalibard, J.; Cohen-Tannoudji, C. (1989). "Laser cooling below the Doppler limit by polarization gradients: simple theoretical models" (https://opg.optica.org/josab/fulltext.cfm?uri=josab-6-11-2023&id=5577). *Journal of the Optical Society of America B*. **6** (11): 2023–2045 – via Optica Publishing Group.
8. Weidemüller, M.; Esslinger, T.; Ol'shanii, M. A.; Hemmerich, A.; Hänsch, T. W. (1994). "A Novel Scheme for Efficient Cooling below the Photon Recoil Limit" (https://iopscience.iop.org/article/10.1209/0295-5075/27/2/006). *EPL*. **27** (109) – via IOP Science.
9. Kerman, Andrew J.; Vuletić, Vladan; Chin, Cheng; Chu, Steven (17 January 2000). "Beyond Optical Molasses: 3D Raman Sideband Cooling of Atomic Cesium to High Phase-Space Density" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.84.439). *Physical Review Letters*. **84** (439) – via APS.

10. Bloch, Immanuel; Dalibard, Jean; Nascimbène, Sylvain (2012). "Quantum simulations with ultracold quantum gases". *Nature Physics*. **8** (4): 267–276. Bibcode:2012NatPh...8..267B (https://ui.adsabs.harvard.edu/abs/2012NatPh...8..267B). doi:10.1038/nphys2259 (https://doi.org/10.1038%2Fnphys2259). S2CID 17023076 (https://api.semanticscholar.org/CorpusID:17023076).

Sources

- Bloch, Immanuel (2008). "Quantum Gases". *Science*. **319** (5867): 1202–1203. Bibcode:2008Sci...319.1202B (https://ui.adsabs.harvard.edu/abs/2008Sci...319.1202B). doi:10.1126/science.1152501 (https://doi.org/10.1126%2Fscience.1152501). PMID 18309072 (https://pubmed.ncbi.nlm.nih.gov/18309072). S2CID 28871617 (https://api.semanticscholar.org/CorpusID:28871617).
- Rousseau, Valery (2010). "Pure Mott Phases in Confined Ultracold Atomic Systems". *Phys. Rev. Lett*. **104** (16): 167201. arXiv:0909.3543 (https://arxiv.org/abs/0909.3543). Bibcode:2010PhRvL.104p7201R (https://ui.adsabs.harvard.edu/abs/2010PhRvL.104p7201R). doi:10.1103/PhysRevLett.104.167201 (https://doi.org/10.1103%2FPhysRevLett.104.167201). PMID 20482076 (https://pubmed.ncbi.nlm.nih.gov/20482076). S2CID 9940436 (https://api.semanticscholar.org/CorpusID:9940436).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Ultracold_atom&oldid=1220176541"

WIKIPEDIA
The Free Encyclopedia

Neutral atom quantum computer

A **neutral atom quantum computer** is a modality of quantum computers built out of Rydberg atoms;[1][2][3][4] this modality has many commonalities with trapped-ion quantum computers. As of December 2023, the concept has been used to demonstrate a 48 logical qubit processor.[5][6]

To perform computation, the atoms are first trapped in a magneto-optical trap.[5] Qubits are then encoded in the energy levels of the atoms. Initialization and operation of the computer is performed via the application of lasers on the qubits.[7] For example, the laser can accomplish arbitrary single qubit gates and a CZ gate for universal quantum computation. The CZ gate is carried out by leveraging the Rydberg blockade which leads to strong interactions when the qubits are physically close to each other. To perform a CZ gate a Rydberg π pulse is applied to the control qubit, a 2π on the target qubit and then a π on the control.[1] Measurement is enforced at the end of the computation with a camera that generates an image of the outcome by measuring the fluorescence of the atoms.[5]

Architecture

Neutral atom quantum computing makes use of several technological advancements in the field laser cooling, magneto-optical trapping and optical tweezers. In one example of the architecture,[8] an array of atoms is loaded into a laser cooled at micro-kelvin temperatures. In each of these atoms, two levels of hyperfine ground subspace are isolated. The qubits are prepared in some initial state using optical pumping. Logic gates are performed using optical or microwave frequency fields and the measurements are done using resonance fluorescence. Most of these architecture are based on Rubidium,[9] Cesium,[10] Ytterbium[11][12] and Strontium[13] atoms.

Single Qubit Gates

Global single qubit gates on all the atoms can be done either by applying a microwave field for qubits encoded in the Hyperfine manifold such as Rb and Cs or by applying an RF magnetic field for qubits encoded in the nuclear spin such as Yb and Sr. Focused laser beams can be used to do single-site one qubit rotation using a lambda-type three level Raman scheme (see figure). In this scheme, the rotation between the qubit states is mediated by an intermediate excited state. Single qubit gate fidelities have been shown to be as high as .999 in state-of-the-art experiments.[14][12][15]

Entangling Gates

To do universal quantum computation, we need at least one two qubit entangling gate.[16] All the gates we talk about in this article are equivalent to a Controlled NOT gate up-to single qubit rotations. Early proposals for doing gates included gates that depended on inter-atomic forces.[2] These forces are weak

and thus the gates were slow. The first fast gate was proposed by Jaksch et al. and made use of the principle of Rydberg Blockade [4](discussed below). Since then, most gates that have been proposed use this principle. We call all such gates Rydberg mediated gates and discuss them below.

Rydberg mediated gates

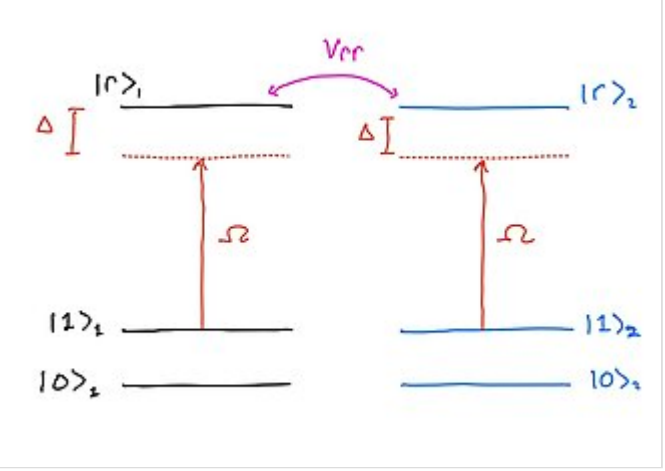
Atoms that have been excited to very large principal quantum number n are known as Rydberg atoms. These highly excited atoms have several desirable properties including high decay life-time and amplified couplings with electromagnetic fields.[17]

The basic principle for Rydberg mediated gates is called the Rydberg blockade.[18] Consider two neutral atoms in their respective ground states. When they are close to each other, their interaction potential is dominated by van Der Waals force $V_{qq} \approx \frac{\mu_B^2}{R^6}$ where μ_B is the Bohr Magneton and R is the distance between the atoms. This interaction is very weak, around 10^{-5} Hz for $R = 10\mu m$. When one of the atoms is put into a Rydberg state (state with very high principal quantum number), the interaction between the two atoms is dominated by second order dipole-dipole interaction which is also weak. When both of the atoms are excited to a Rydberg state, then the resonant dipole-dipole interaction becomes $V_{rr} = \frac{(n^2 e a_0)^2}{R^3}$ where a_0 is the Bohr radius. This interaction is around 100MHz at $R = 10\mu m$, around twelve orders of magnitude larger. This interaction potential induces a blockade, where-in, if one atom is excited to a Rydberg state, the other nearby atoms cannot be excited to a Rydberg state because the two-atom Rydberg state is far detuned. This phenomena is called the Rydberg blockade. Rydberg mediated gates make use of this blockade as a control mechanism to implement two qubit controlled gates.

Let's consider the physics induced by the this blockade. Suppose we are considering two isolated neutral atoms in a magneto-optical trap. Ignoring the coupling of hyperfine levels that make the qubit and motional degrees of freedom, the Hamiltonian of this system can be written as:

$$H = H_1 + H_2 + V_{rr}|r\rangle_1\langle r| \otimes |r\rangle_2\langle r|)$$

where,
$H_i = \frac{1}{2}((\Omega|1\rangle_i\langle r| + \Omega^*|r\rangle_i\langle 1|) - \Delta|r\rangle_i\langle r|$ is the Hamiltonian of i-th atom, Ω is the Rabi frequency of coupling between the Rydberg states and the $|1\rangle$ state and Δ is the detuning (see figure to the right for level diagram). When $|V_{rr}| >> |\Omega|, |\Delta|$, we are in the so-called Rydberg Blockade regime. In this regime, the $|rr\rangle$ state is highly detuned from the rest of the system and thus is effectively decoupled. For the rest of this article, we consider only the Rydberg Blockade regime.

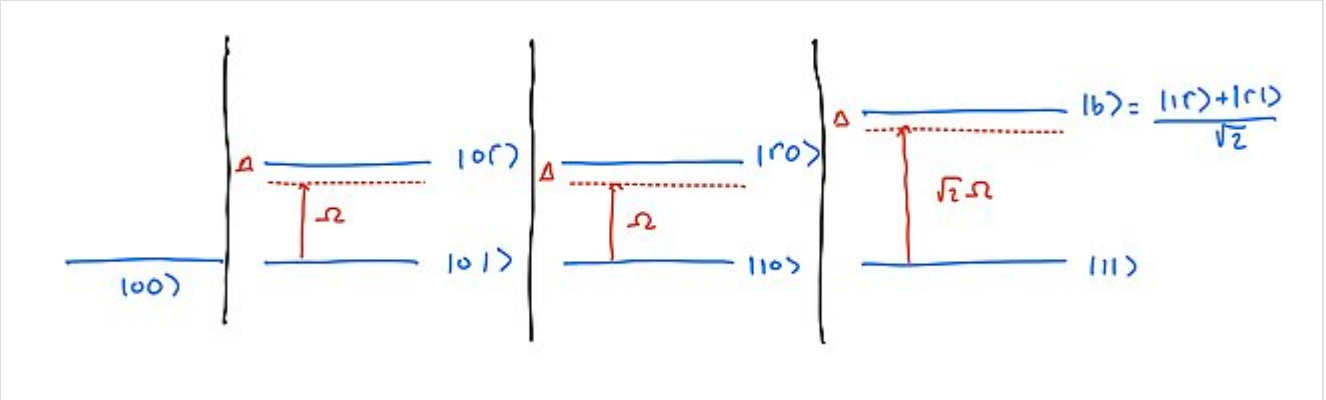


Level diagram of the Hamiltonian of two neutral atoms interacting via Rydberg interaction. The $|1\rangle$ states are coupled with $|r\rangle$ states in each atom.

The physics of this Hamiltonian can be divided into several subspaces depending on the initial state. The $|00\rangle$ state is decoupled and does not evolve. Suppose only the i-th the atom is in $|1\rangle$ state ($|10\rangle$, $|01\rangle$), then the Hamiltonian is given by $\boldsymbol{H_i}$. This Hamiltonian is the standard two-level Rabi hamiltonian. It characterizes the "light shift" in a two level system and has eigenvalues $E_{LS}^{(1)} = \frac{1}{2}(\Delta \pm \sqrt{\Omega^2 + \Delta^2})$.

If both atoms are in the excited state $|11\rangle$ the effective system evolves in the subspace of $\{|1r\rangle, |r1\rangle, |11\rangle\}$. It is convenient to rewrite the Hamiltonian in terms of bright $|b\rangle = \frac{1}{\sqrt{2}}(|r1\rangle + |1r\rangle)$ and dark $|d\rangle = \frac{1}{\sqrt{2}}(|r1\rangle - |1r\rangle)$ basis states, along with $|11\rangle$. In this basis, the Hamiltonian is given by

$$H = -\Delta(|b\rangle\langle b| + |d\rangle\langle d|) + \frac{\sqrt{2}}{2}(\Omega|b\rangle\langle 11| + \Omega^*|11\rangle\langle b|).$$



Level diagram of different subspaces that interact with each other in a Rydberg Hamiltonian under the blockade regime. The black lines show the separation between subspaces that do not interact with each other directly.

Note that the dark state is decoupled from the bright state and the $|11\rangle$ state. Thus we can ignore it and the effective evolution reduces to a two-level system consisting of the bright state and $|11\rangle$ state. In this basis, the dressed eigenvalues and eigenvectors of the hamiltonian are given by:

$$E_{LS}^{(2)} = \frac{1}{2}(\Delta \pm \sqrt{2\Omega^2 + \Delta^2})$$

$$|\tilde{11}\rangle = \cos(\theta/2)|11\rangle + \sin(\theta/2)|b\rangle$$

$$|\tilde{b}\rangle = \cos(\theta/2)|b\rangle - \sin(\theta/2)|11\rangle,$$

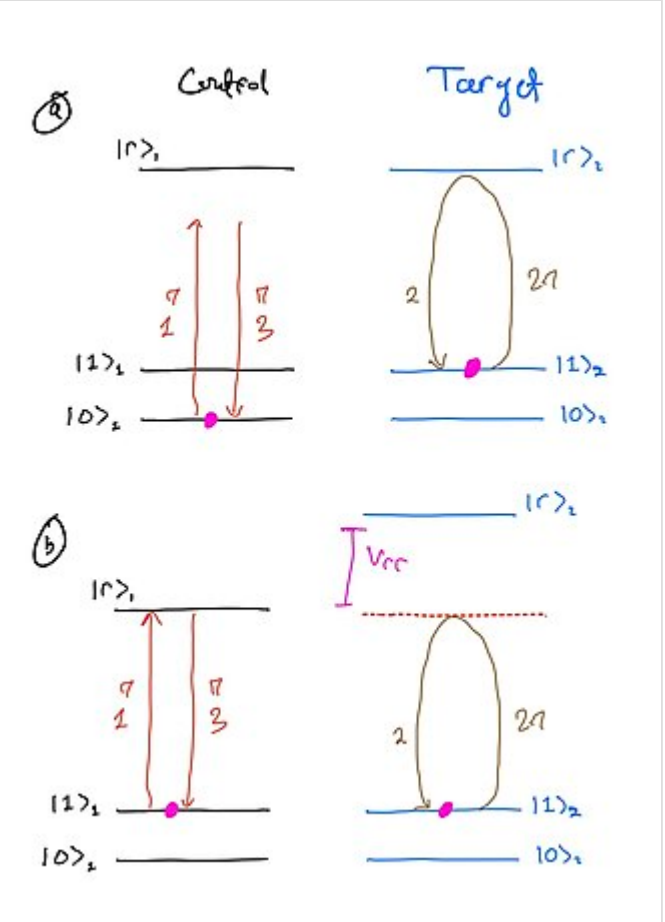
where, θ depends on the Rabi frequency and detuning. We will make use of these considerations in the gates below. The level diagrams of these subspaces have been shown in the figure above.

Jaksch Gate

We can use the Rydberg blockade to implement a controlled-phase gate by applying standard Rabi pulses between the $|1\rangle$ and $|r\rangle$ levels. Consider the following protocol:[4]

1. Apply π pulse to control atom (red).
2. Apply 2π pulse the target atom (brown).
3. Apply π pulse to control atom again (red).

The figure on the right shows what this pulse sequence does. When the state is $|00\rangle$, both levels are uncoupled from the Rydberg states and so the pulses do nothing. When either of the atoms is in $|0\rangle$ state, the other one picks up a -1 phase due to the 2π pulse. When the state is $|11\rangle$, the second atom is off-resonant to its Rydberg state and thus does not pick up any phase, however the first one does. The truth table of this gate is given below. This is equivalent to a controlled-z gate up-to a local rotation to the hyperfine levels.



Pictorial representation of the Jaksch Gate. a)Effect of pulse sequences(labelled by numbers) when the control qubit is in $|0\rangle$ state. b)Effect when the control qubit is in $|1\rangle$state.

Truth Table of Jaksch-Gate

Initial State	Final State
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$-\|01\rangle$
$\|10\rangle$	$-\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

Adiabatic Gate

The adiabatic gate was introduced as an alternative to the Jaksch gate.[19] It is global and symmetric and thus it does not require locally focused lasers. Moreover, the Adiabatic Gate prevents the problem of spurious phase accumulation when the atom is in Rydberg state. In the Adiabatic Gate, instead of doing fast pulses, we dress the atom with an adiabatic pulse sequence that takes the atom on a trajectory around the Bloch sphere and back. The levels pick up a phase on this trip due to the so-called "light shift" induced by the lasers. The shapes of pulses can be chosen to control this phase.

If both atoms are in the $|00\rangle$ state, nothing happens so $|00\rangle \rightarrow |00\rangle$. If one of them is in the $|0\rangle$ state, the other atom picks up a phase due to light shift: $|01\rangle \rightarrow e^{i\phi_1}|01\rangle$ and similarly $|10\rangle \rightarrow e^{i\phi_1}|10\rangle$ with:

$$\phi_1 = \int E_{LS}^{(1)}(t)dt = \int \frac{1}{2}(\Delta(t) - \sqrt{\Omega^2(t) + \Delta^2(t)})dt.$$

When both of the atoms are in $|1\rangle$ states, the atoms pick up a phase due to the two-atom light shift as seen by the eigenvalues of Hamiltonian above, then $|11\rangle \rightarrow e^{i\phi_2}|11\rangle$ with

$$\phi_2 = \int E_{LS}^{(2)}(t)dt = \int \frac{1}{2}(\Delta(t) - \sqrt{2\Omega^2(t) + \Delta^2(t)})dt.$$

Note that this light shift is not equal to twice the single atom light shifts. The single atom light-shifts are then cancelled by a global pulse that implements $U = \exp(-i\phi_1|1\rangle\langle 1|)$ to get rid of the single qubit light shifts. The truth table for this gate is given to the right. This protocol leaves a total phase of

$\int (E_{LS}^{(2)}(t) - 2E_{LS}^{(1)}(t))dt$ phase on the $|11\rangle$ state. We can choose the pulses so that this phase equals π, making it a controlled-Z gate. An extension to this gate was introduced to make it robust against errors in reference.[20]

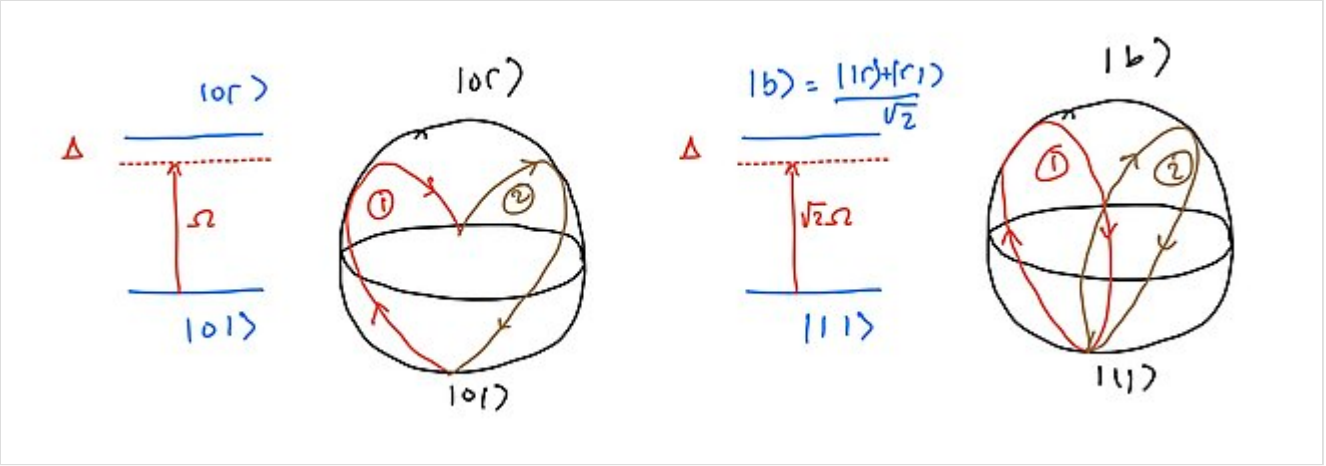
Truth Table of Adiabatic-Gate

Initial State	Final State
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$e^{i(\phi_2 - 2\phi_1)}\|11\rangle$

Levine-Pichler Gate

The adiabatic gate is global but it is slow (due to adiabatic condition). The Levine-Pichler gate was introduced as a fast diabatic substitute to the global Adiabatic Gate.[21] This gate uses carefully chosen pulse sequences to perform a controlled-phase gate. In this protocol, we apply the following pulse sequence:

1. Apply pulse of length $\tau = 2\pi/\sqrt{\Delta^2 + 2\Omega^2}$ with Rabi frequency Ω (red).
2. Apply another pulse of length $\tau = 2\pi/\sqrt{\Delta^2 + 2\Omega^2}$ but with a phase shifted Rabi frequency $\Omega \to e^{-i\xi}\Omega$ (brown).



Levine Pitcher gate on the Bloch sphere.

The intuition of this gate is best understood in terms of the picture given above. When the state of the system is $|11\rangle$, the pulses send the state around the Bloch sphere twice and accumulates a net phase $\phi_2 = \dfrac{4\pi\Delta}{\sqrt{\Delta^2 + 2\Omega^2}}$. When one of the atoms is in $|0\rangle$ state, the other atom does not go around the Bloch sphere fully after the first pulse due to the mismatch in Rabi frequency. The second pulse corrects for this effect by rotating the state around a different axis. This puts the atom back into the $|1\rangle$ state with a net phase ϕ_1, which can be calculated easily. The pulses can be chosen to make $e^{i\phi_2} = e^{i(2\phi_1 + \pi)}$. Doing so makes this gate equivalent to a controlled-z gate up-to a local rotation. The truth table of Levine-Pichler gate is given on the right. This gate has been improved using the methods of quantum optimal controls recently.[22][23]

Truth Table of Levine-Pichler Gate

Initial State	Final State
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$e^{i\phi_1}\|01\rangle$
$\|10\rangle$	$e^{i\phi_1}\|10\rangle$
$\|11\rangle$	$e^{i(2\phi_1 + \pi)}\|11\rangle$

Entangling gates in state-of-the art neutral atom quantum computing platforms have been implemented with up-to .995 quantum fidelity.[9]

See also

- Superconducting quantum computing
- Trapped-ion quantum computer

References

1. Saffman, Mark; Walker, Thad G; Klaus, Mølmer (2010). "Quantum information with Rydberg atoms" (https://link.aps.org/doi/10.1103/RevModPhys.82.2313). *Rev. Mod. Phys*. **82** (3): 2313–2363. arXiv:0909.4777 (https://arxiv.org/abs/0909.4777). Bibcode:2010RvMP...82.2313S (https://ui.adsabs.harvard.edu/abs/2010RvMP...82.2313S). doi:10.1103/RevModPhys.82.2313 (https://doi.org/10.1103%2FRevModPhys.82.2313). S2CID 14285764 (https://api.semanticscholar.org/CorpusID:14285764).
2. Brennen, Gavin K.; Caves, Carlton M.; Jessen, Poul S.; Deutsch, Ivan H. (1 February 1999). "Quantum Logic Gates in Optical Lattices" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.82.1060). *Physical Review Letters*. **82** (5): 1060–1063. arXiv:quant-ph/9806021 (https://arxiv.org/abs/quant-ph/9806021). Bibcode:1999PhRvL..82.1060B (https://ui.adsabs.harvard.edu/abs/1999PhRvL..82.1060B). doi:10.1103/PhysRevLett.82.1060 (https://doi.org/10.1103%2FPhysRevLett.82.1060).
3. Briegel, H.-J.; Calarco, T.; Jaksch, D.; Cirac, J. I.; Zoller, P. (February 2000). "Quantum computing with neutral atoms" (https://www.tandfonline.com/doi/abs/10.1080/09500340008244052). *Journal of Modern Optics*. **47** (2–3): 415–451. arXiv:quant-ph/9904010 (https://arxiv.org/abs/quant-ph/9904010). Bibcode:2000JMOp...47..415B (https://ui.adsabs.harvard.edu/abs/2000JMOp...47..415B). doi:10.1080/09500340008244052 (https://doi.org/10.1080%2F09500340008244052). ISSN 0950-0340 (https://search.worldcat.org/issn/0950-0340).
4. Jaksch, D.; Cirac, J. I.; Zoller, P.; Rolston, S. L.; Côté, R.; Lukin, M. D. (4 September 2000). "Fast Quantum Gates for Neutral Atoms" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.2208). *Physical Review Letters*. **85** (10): 2208–2211. arXiv:quant-ph/0004038 (https://arxiv.org/abs/quant-ph/0004038). Bibcode:2000PhRvL..85.2208J (https://ui.adsabs.harvard.edu/abs/2000PhRvL..85.2208J). doi:10.1103/PhysRevLett.85.2208 (https://doi.org/10.1103%2FPhysRevLett.85.2208). PMID 10970499 (https://pubmed.ncbi.nlm.nih.gov/10970499).
5. Bluvstein, Dolev; Evered, Simon J.; Geim, Alexandra A.; Li, Sophie H.; Zhou, Hengyun; Manovitz, Tom; Ebadi, Sepehr; Cain, Madelyn; Kalinowski, Marcin; Hangleiter, Dominik; Bonilla Ataides, J. Pablo; Maskara, Nishad; Cong, Iris; Gao, Xun; Sales Rodriguez, Pedro (2024-02-01). "Logical quantum processor based on reconfigurable atom arrays" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). *Nature*. **626** (7997): 58–65. arXiv:2312.03982 (https://arxiv.org/abs/2312.03982). Bibcode:2024Natur.626...58B (https://ui.adsabs.harvard.edu/abs/2024Natur.626...58B). doi:10.1038/s41586-023-06927-3 (https://doi.org/10.1038%2Fs41586-023-06927-3). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMC 10830422 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10830422). PMID 38056497 (https://pubmed.ncbi.nlm.nih.gov/38056497).
6. Yirka, Bob (2023-12-07). "Using logical qubits to make a quantum computer that can correct its errors" (https://phys.org/news/2023-12-logical-qubits-quantum-errors.html). Retrieved 2024-02-10.

7. Genkina, Dina (2013-10-18). "Neutral-atom quantum computers are having a moment" (https://physicsworld.com/a/neutral-atom-quantum-computers-are-having-a-moment/). Retrieved 2013-10-18.
8. Saffman, M (28 October 2016). "Quantum computing with atomic qubits and Rydberg interactions: progress and challenges" (https://iopscience.iop.org/article/10.1088/0953-4075/49/20/202001). *Journal of Physics B: Atomic, Molecular and Optical Physics*. **49** (20): 202001. arXiv:1605.05207 (https://arxiv.org/abs/1605.05207). Bibcode:2016JPhB...49t2001S (https://ui.adsabs.harvard.edu/abs/2016JPhB...49t2001S). doi:10.1088/0953-4075/49/20/202001 (https://doi.org/10.1088%2F0953-4075%2F49%2F20%2F202001). ISSN 0953-4075 (https://search.worldcat.org/issn/0953-4075).
9. Evered, Simon J.; Bluvstein, Dolev; Kalinowski, Marcin; Ebadi, Sepehr; Manovitz, Tom; Zhou, Hengyun; Li, Sophie H.; Geim, Alexandra A.; Wang, Tout T.; Maskara, Nishad; Levine, Harry; Semeghini, Giulia; Greiner, Markus; Vuletić, Vladan; Lukin, Mikhail D. (October 2023). "High-fidelity parallel entangling gates on a neutral-atom quantum computer" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10567572). *Nature*. **622** (7982): 268–272. arXiv:2304.05420 (https://arxiv.org/abs/2304.05420). Bibcode:2023Natur.622..268E (https://ui.adsabs.harvard.edu/abs/2023Natur.622..268E). doi:10.1038/s41586-023-06481-y (https://doi.org/10.1038%2Fs41586-023-06481-y). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 10567572 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10567572). PMID 37821591 (https://pubmed.ncbi.nlm.nih.gov/37821591).
10. Graham, T. M.; Song, Y.; Scott, J.; Poole, C.; Phuttitarn, L.; Jooya, K.; Eichler, P.; Jiang, X.; Marra, A.; Grinkemeyer, B.; Kwon, M.; Ebert, M.; Cherek, J.; Lichtman, M. T.; Gillette, M.; Gilbert, J.; Bowman, D.; Ballance, T.; Campbell, C.; Dahl, E. D.; Crawford, O.; Blunt, N. S.; Rogers, B.; Noel, T.; Saffman, M. (April 2022). "Multi-qubit entanglement and algorithms on a neutral-atom quantum computer" (https://www.nature.com/articles/s41586-022-04603-6#Sec6). *Nature*. **604** (7906): 457–462. arXiv:2112.14589 (https://arxiv.org/abs/2112.14589). Bibcode:2022Natur.604..457G (https://ui.adsabs.harvard.edu/abs/2022Natur.604..457G). doi:10.1038/s41586-022-04603-6 (https://doi.org/10.1038%2Fs41586-022-04603-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 35444321 (https://pubmed.ncbi.nlm.nih.gov/35444321).
11. Jenkins, Alec; Lis, Joanna W.; Senoo, Aruku; McGrew, William F.; Kaufman, Adam M. (3 May 2022). "Ytterbium Nuclear-Spin Qubits in an Optical Tweezer Array" (https://journals.aps.org/prx/abstract/10.1103/PhysRevX.12.021027). *Physical Review X*. **12** (2): 021027. arXiv:2112.06732 (https://arxiv.org/abs/2112.06732). Bibcode:2022PhRvX..12b1027J (https://ui.adsabs.harvard.edu/abs/2022PhRvX..12b1027J). doi:10.1103/PhysRevX.12.021027 (https://doi.org/10.1103%2FPhysRevX.12.021027).
12. Ma, S.; Burgers, A. P.; Liu, G.; Wilson, J.; Zhang, B.; Thompson, J. D. (3 May 2022). "Universal Gate Operations on Nuclear Spin Qubits in an Optical Tweezer Array of 171Yb Atoms" (https://journals.aps.org/prx/abstract/10.1103/PhysRevX.12.021028). *Physical Review X*. **12** (2): 021028. arXiv:2112.06799 (https://arxiv.org/abs/2112.06799). doi:10.1103/PhysRevX.12.021028 (https://doi.org/10.1103%2FPhysRevX.12.021028).
13. Madjarov, Ivaylo S.; Covey, Jacob P.; Shaw, Adam L.; Choi, Joonhee; Kale, Anant; Cooper, Alexandre; Pichler, Hannes; Schkolnik, Vladimir; Williams, Jason R.; Endres, Manuel (August 2020). "High-fidelity entanglement and detection of alkaline-earth Rydberg atoms" (https://www.nature.com/articles/s41567-020-0903-z). *Nature Physics*. **16** (8): 857–861. arXiv:2001.04455 (https://arxiv.org/abs/2001.04455). Bibcode:2020NatPh..16..857M (https://ui.adsabs.harvard.edu/abs/2020NatPh..16..857M). doi:10.1038/s41567-020-0903-z (https://doi.org/10.1038%2Fs41567-020-0903-z). ISSN 1745-2481 (https://search.worldcat.org/issn/1745-2481).

14. Graham, T. M.; Song, Y.; Scott, J.; Poole, C.; Phuttitarn, L.; Jooya, K.; Eichler, P.; Jiang, X.; Marra, A.; Grinkemeyer, B.; Kwon, M.; Ebert, M.; Cherek, J.; Lichtman, M. T.; Gillette, M.; Gilbert, J.; Bowman, D.; Ballance, T.; Campbell, C.; Dahl, E. D.; Crawford, O.; Blunt, N. S.; Rogers, B.; Noel, T.; Saffman, M. (April 2022). "Multi-qubit entanglement and algorithms on a neutral-atom quantum computer" (https://www.nature.com/articles/s41586-022-04603-6). *Nature*. **604** (7906): 457–462. arXiv:2112.14589 (https://arxiv.org/abs/2112.14589). Bibcode:2022Natur.604..457G (https://ui.adsabs.harvard.edu/abs/2022Natur.604..457G). doi:10.1038/s41586-022-04603-6 (https://doi.org/10.1038%2Fs41586-022-04603-6). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 35444321 (https://pubmed.ncbi.nlm.nih.gov/35444321).
15. Xia, T.; Lichtman, M.; Maller, K.; Carr, A. W.; Piotrowicz, M. J.; Isenhower, L.; Saffman, M. (12 March 2015). "Randomized Benchmarking of Single-Qubit Gates in a 2D Array of Neutral-Atom Qubits" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.114.100503). *Physical Review Letters*. **114** (10): 100503. arXiv:1501.02041 (https://arxiv.org/abs/1501.02041). Bibcode:2015PhRvL.114j0503X (https://ui.adsabs.harvard.edu/abs/2015PhRvL.114j0503X). doi:10.1103/PhysRevLett.114.100503 (https://doi.org/10.1103%2FPhysRevLett.114.100503). PMID 25815916 (https://pubmed.ncbi.nlm.nih.gov/25815916).
16. Nielsen, Michael A.; Chuang, Isaac L. (9 December 2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition* (https://www.cambridge.org/highereducation/books/quantum-computation-and-quantum-information/01E10196D0A682A6AEFFEA52D53BE9AE#overview). doi:10.1017/CBO9780511976667 (https://doi.org/10.1017%2FCBO9780511976667). ISBN 978-1-107-00217-3.
17. Saffman, M.; Walker, T. G.; Mølmer, K. (18 August 2010). "Quantum information with Rydberg atoms" (https://journals.aps.org/rmp/abstract/10.1103/RevModPhys.82.2313). *Reviews of Modern Physics*. **82** (3): 2313–2363. arXiv:0909.4777 (https://arxiv.org/abs/0909.4777). Bibcode:2010RvMP...82.2313S (https://ui.adsabs.harvard.edu/abs/2010RvMP...82.2313S). doi:10.1103/RevModPhys.82.2313 (https://doi.org/10.1103%2FRevModPhys.82.2313).
18. Walker, Thad G.; Saffman, Mark (1 July 2012). "Chapter 2 - Entanglement of Two Atoms Using Rydberg Blockade" (https://www.sciencedirect.com/science/article/abs/pii/B9780123964823000028). *Advances in Atomic, Molecular, and Optical Physics*. **61**. Academic Press: 81–115. arXiv:1202.5328 (https://arxiv.org/abs/1202.5328). doi:10.1016/B978-0-12-396482-3.00002-8 (https://doi.org/10.1016%2FB978-0-12-396482-3.00002-8). ISBN 978-0-12-396482-3.
19. Keating, Tyler; Cook, Robert L.; Hankin, Aaron M.; Jau, Yuan-Yu; Biedermann, Grant W.; Deutsch, Ivan H. (28 January 2015). "Robust quantum logic in neutral atoms via adiabatic Rydberg dressing" (https://journals.aps.org/pra/abstract/10.1103/PhysRevA.91.012337). *Physical Review A*. **91** (1): 012337. arXiv:1411.2622 (https://arxiv.org/abs/1411.2622). Bibcode:2015PhRvA..91a2337K (https://ui.adsabs.harvard.edu/abs/2015PhRvA..91a2337K). doi:10.1103/PhysRevA.91.012337 (https://doi.org/10.1103%2FPhysRevA.91.012337).
20. Mitra, Anupam; Martin, Michael J.; Biedermann, Grant W.; Marino, Alberto M.; Poggi, Pablo M.; Deutsch, Ivan H. (20 March 2020). "Robust M\o{}lmer-S\o{}rensen gate for neutral atoms using rapid adiabatic Rydberg dressing" (https://journals.aps.org/pra/abstract/10.1103/PhysRevA.101.030301). *Physical Review A*. **101** (3): 030301. arXiv:1911.04045 (https://arxiv.org/abs/1911.04045). doi:10.1103/PhysRevA.101.030301 (https://doi.org/10.1103%2FPhysRevA.101.030301).
21. Levine, Harry; Keesling, Alexander; Semeghini, Giulia; Omran, Ahmed; Wang, Tout T.; Ebadi, Sepehr; Bernien, Hannes; Greiner, Markus; Vuletić, Vladan; Pichler, Hannes; Lukin, Mikhail D. (22 October 2019). "Parallel Implementation of High-Fidelity Multiqubit Gates with Neutral Atoms" (https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.123.170503). *Physical Review Letters*. **123** (17): 170503. arXiv:1908.06101 (https://arxiv.org/abs/1908.06101). Bibcode:2019PhRvL.123q0503L (https://ui.adsabs.harvard.edu/abs/2019PhRvL.123q0503L). doi:10.1103/PhysRevLett.123.170503 (https://doi.org/10.1103%2FPhysRevLett.123.170503). PMID 31702233 (https://pubmed.ncbi.nlm.nih.gov/31702233).

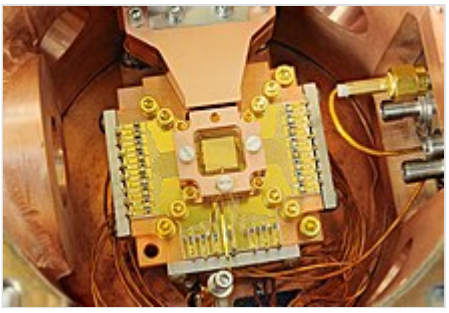
22. Pagano, Alice; Weber, Sebastian; Jaschke, Daniel; Pfau, Tilman; Meinert, Florian; Montangero, Simone; Büchler, Hans Peter (11 July 2022). "Error budgeting for a controlled-phase gate with strontium-88 Rydberg atoms" (https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.4.033019). *Physical Review Research*. **4** (3): 033019. arXiv:2202.13849 (https://arxiv.org/abs/2202.13849). Bibcode:2022PhRvR...4c3019P (https://ui.adsabs.harvard.edu/abs/2022PhRvR...4c3019P). doi:10.1103/PhysRevResearch.4.033019 (https://doi.org/10.1103%2FPhysRevResearch.4.033019).
23. Jandura, Sven; Pupillo, Guido (13 May 2022). "Time-Optimal Two- and Three-Qubit Gates for Rydberg Atoms" (https://quantum-journal.org/papers/q-2022-05-13-712/). *Quantum*. **6**: 712. arXiv:2202.00903 (https://arxiv.org/abs/2202.00903). Bibcode:2022Quant...6..712J (https://ui.adsabs.harvard.edu/abs/2022Quant...6..712J). doi:10.22331/q-2022-05-13-712 (https://doi.org/10.22331%2Fq-2022-05-13-712).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Neutral_atom_quantum_computer&oldid=1244543032"

WIKIPEDIA
The Free Encyclopedia

Trapped-ion quantum computer

A **trapped-ion quantum computer** is one proposed approach to a large-scale quantum computer. Ions, or charged atomic particles, can be confined and suspended in free space using electromagnetic fields. Qubits are stored in stable electronic states of each ion, and quantum information can be transferred through the collective quantized motion of the ions in a shared trap (interacting through the Coulomb force). Lasers are applied to induce coupling between the qubit states (for single qubit operations) or coupling between the internal qubit states and the external motional states (for entanglement between qubits).[1]



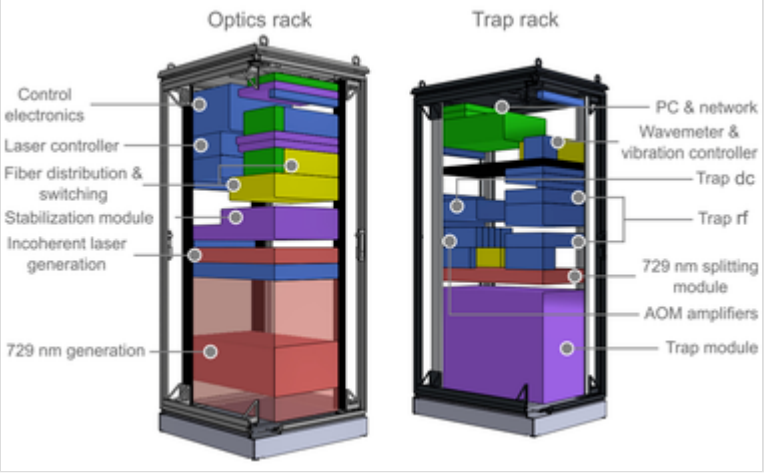
Chip ion trap for quantum computing from 2011 at NIST

The fundamental operations of a quantum computer have been demonstrated experimentally with the currently highest accuracy in trapped-ion systems. Promising schemes in development to scale the system to arbitrarily large numbers of qubits include transporting ions to spatially distinct locations in an array of ion traps, building large entangled states via photonically connected networks of remotely entangled ion chains, and combinations of these two ideas. This makes the trapped-ion quantum computer system one of the most promising architectures for a scalable, universal quantum computer. As of December 2023, the largest number of particles to be controllably entangled is 32 trapped ions.[2]

History

The first implementation scheme for a controlled-NOT quantum gate was proposed by Ignacio Cirac and Peter Zoller in 1995,[3] specifically for the trapped-ion system. The same year, a key step in the controlled-NOT gate was experimentally realized at NIST Ion Storage Group, and research in quantum computing began to take off worldwide.

In 2021, researchers from the University of Innsbruck presented a quantum computing demonstrator that fits inside two 19-inch server racks, the world's first quality standards-meeting compact trapped-ion quantum computer.[5][4]

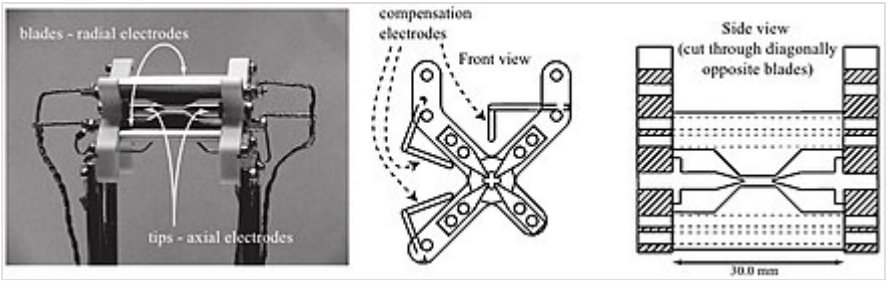


Simplified scale model[4]

Paul trap

The electrodynamic quadrupole ion trap currently used in trapped-ion quantum computing research was invented in the 1950s by Wolfgang Paul (who received

the Nobel Prize for his work in 1989[6]). Charged particles cannot be trapped in 3D by just electrostatic forces because of Earnshaw's theorem. Instead, an electric field oscillating at radio frequency (RF) is applied, forming a potential with the shape of a saddle spinning at the RF frequency. If the RF field has the right parameters (oscillation frequency and field strength), the charged particle becomes effectively trapped at the saddle point by a restoring force, with the motion described by a set of Mathieu equations.[1]



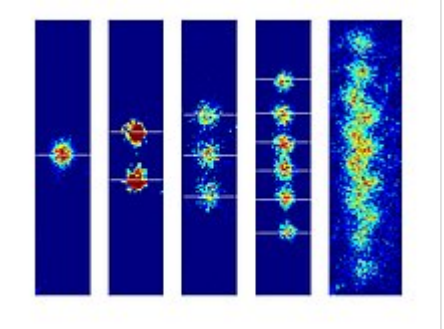
Classical linear Paul trap in Innsbruck for a string of calcium ions

This saddle point is the point of minimized energy magnitude, $|\boldsymbol{E}(\mathbf{x})|$, for the ions in the potential field.[7] The Paul trap is often described as a harmonic potential well that traps ions in two dimensions (assume $\hat{\boldsymbol{x}}$ and $\hat{\boldsymbol{y}}$ without loss of generality) and does not trap ions in the $\hat{\boldsymbol{z}}$ direction. When multiple ions are at the saddle point and the system is at equilibrium, the ions are only free to move in $\hat{\boldsymbol{z}}$. Therefore, the ions will repel each other and create a vertical configuration in $\hat{\boldsymbol{z}}$, the simplest case being a linear strand of only a few ions.[8][9][10][11] Coulomb interactions of increasing complexity will create a more intricate ion configuration if many ions are initialized in the same trap.[1][10] Furthermore, the additional vibrations of the added ions greatly complicate the quantum system, which makes initialization and computation more difficult.[11]

Once trapped, the ions should be cooled such that $k_{\mathrm{B}}T \ll \hbar\omega_z$ (see Lamb Dicke regime). This can be achieved by a combination of Doppler cooling and resolved sideband cooling. At this very low temperature, vibrational energy in the ion trap is quantized into phonons by the energy eigenstates of the ion strand, which are called the center of mass vibrational modes. A single phonon's energy is given by the relation $\hbar\omega_z$. These quantum states occur when the trapped ions vibrate together and are completely isolated from the external environment. If the ions are not properly isolated, noise can result from ions interacting with external electromagnetic fields, which creates random movement and destroys the quantized energy states.[1]

Requirements for quantum computation

The full requirements for a functional quantum computer are not entirely known, but there are many generally accepted requirements. David DiVincenzo outlined several of these criteria for quantum computing.[1]


Magnesium ions in a trap

Qubits

Any two-level quantum system can form a qubit, and there are two predominant ways to form a qubit using the electronic states of an ion:

1. Two ground state hyperfine levels (these are called "hyperfine qubits")
2. A ground state level and an excited level (these are called the "optical qubits")

Hyperfine qubits are extremely long-lived (decay time of the order of thousands to millions of years) and phase/frequency stable (traditionally used for atomic frequency standards).[11] Optical qubits are also relatively long-lived (with a decay time of the order of a second), compared to the logic gate operation time (which is of the order of microseconds). The use of each type of qubit poses its own distinct challenges in the laboratory.

Initialization

Ionic qubit states can be prepared in a specific qubit state using a process called optical pumping. In this process, a laser couples the ion to some excited states which eventually decay to one state which is not coupled to the laser. Once the ion reaches that state, it has no excited levels to couple to in the presence of that laser and, therefore, remains in that state. If the ion decays to one of the other states, the laser will continue to excite the ion until it decays to the state that does not interact with the laser. This initialization process is standard in many physics experiments and can be performed with extremely high fidelity (>99.9%).[12]

The system's initial state for quantum computation can therefore be described by the ions in their hyperfine and motional ground states, resulting in an initial center of mass phonon state of $|0\rangle$ (zero phonons).[1]

Measurement

Measuring the state of the qubit stored in an ion is quite simple. Typically, a laser is applied to the ion that couples only one of the qubit states. When the ion collapses into this state during the measurement process, the laser will excite it, resulting in a photon being released when the ion decays from the excited state. After decay, the ion is continually excited by the laser and repeatedly emits photons. These photons can be collected by a photomultiplier tube (PMT) or a charge-coupled device (CCD) camera. If the ion collapses into the other qubit state, then it does not interact with the laser and no photon is emitted. By counting the number of collected photons, the state of the ion may be determined with a very high accuracy (>99.99%).[13]

Arbitrary single qubit rotation

One of the requirements of universal quantum computing is to coherently change the state of a single qubit. For example, this can transform a qubit starting out in 0 into any arbitrary superposition of 0 and 1 defined by the user. In a trapped-ion system, this is often done using magnetic dipole transitions or stimulated Raman transitions for hyperfine qubits and electric quadrupole transitions for optical qubits. The term "rotation" alludes to the Bloch sphere representation of a qubit pure state. Gate fidelity can be greater than 99%.

The rotation operators $R_x(\theta)$ and $R_y(\theta)$ can be applied to individual ions by manipulating the frequency of an external electromagnetic field from and exposing the ions to the field for specific amounts of time. These controls create a Hamiltonian of the form $H_I^i = \hbar\Omega/2(S_+ \exp(i\phi) + S_- \exp(-i\phi))$. Here, S_+ and S_- are the raising and lowering operators of spin (see Ladder operator). These rotations are the universal building blocks for single-qubit gates in quantum computing.[1]

To obtain the Hamiltonian for the ion-laser interaction, apply the Jaynes–Cummings model. Once the Hamiltonian is found, the formula for the unitary operation performed on the qubit can be derived using the principles of quantum time evolution. Although this model utilizes the rotating wave approximation, it proves to be effective for the purposes of trapped-ion quantum computing.[1]

Two qubit entangling gates

Besides the controlled-NOT gate proposed by Cirac and Zoller in 1995, many equivalent, but more robust, schemes have been proposed and implemented experimentally since. Recent theoretical work by JJ. Garcia-Ripoll, Cirac, and Zoller have shown that there are no fundamental limitations to the speed of entangling gates, but gates in this impulsive regime (faster than 1 microsecond) have not yet been demonstrated experimentally. The fidelity of these implementations has been greater than 99%.[14]

Scalable trap designs

Quantum computers must be capable of initializing, storing, and manipulating many qubits at once in order to solve difficult computational problems. However, as previously discussed, a finite number of qubits can be stored in each trap while still maintaining their computational abilities. It is therefore necessary to design interconnected ion traps that are capable of transferring information from one trap to another. Ions can be separated from the same interaction region to individual storage regions and brought back together without losing the quantum information stored in their internal states. Ions can also be made to turn corners at a "T" junction, allowing a two dimensional trap array design. Semiconductor fabrication techniques have also been employed to manufacture the new generation of traps, making the 'ion trap on a chip' a reality. An example is the quantum charge-coupled device (QCCD) designed by D. Kielpinski, Christopher Monroe and David J. Wineland.[15] QCCDs resemble mazes of electrodes with designated areas for storing and manipulating qubits.

The variable electric potential created by the electrodes can both trap ions in specific regions and move them through the transport channels, which negates the necessity of containing all ions in a single trap. Ions in the QCCD's memory region are isolated from any operations and therefore the information contained in their states is kept for later use. Gates, including those that entangle two ion states, are applied to qubits in the interaction region by the method already described in this article.[15]

Decoherence in scalable traps

When an ion is being transported between regions in an interconnected trap and is subjected to a nonuniform magnetic field, decoherence can occur in the form of the equation below (see Zeeman effect).[15] This effectively changes the relative phase of the quantum state. The up and down arrows correspond to a general superposition qubit state, in this case the ground and excited states of the ion.

$$|\uparrow\rangle + |\downarrow\rangle \longrightarrow \mathbf{exp}(i\alpha)\,|\uparrow\rangle + |\downarrow\rangle$$

Additional relative phases could arise from physical movements of the trap or the presence of unintended electric fields. If the user could determine the parameter α, accounting for this decoherence would be relatively simple, as known quantum information processes exist for correcting a relative phase.[1] However, since α from the interaction with the magnetic field is path-dependent, the problem is highly

complex. Considering the multiple ways that decoherence of a relative phase can be introduced in an ion trap, reimagining the ion state in a new basis that minimizes decoherence could be a way to eliminate the issue.

One way to combat decoherence is to represent the quantum state in a new basis called the decoherence-free subspaces, or DFS., with basis states $|\uparrow\downarrow\rangle$ and $|\downarrow\uparrow\rangle$. The DFS is actually the subspace of two ion states, such that if both ions acquire the same relative phase, the total quantum state in the DFS will be unaffected.[15]

Challenges

Trapped-ion quantum computers theoretically meet all of DiVincenzo's criteria for quantum computing, but implementation of the system can be quite difficult. The main challenges facing trapped-ion quantum computing are the initialization of the ion's motional states, and the relatively brief lifetimes of the phonon states.[1] Decoherence also proves to be challenging to eliminate, and is caused when the qubits interact with the external environment undesirably.[3]

CNOT gate implementation

The controlled NOT gate is a crucial component for quantum computing, as any quantum gate can be created by a combination of CNOT gates and single-qubit rotations.[11] It is therefore important that a trapped-ion quantum computer can perform this operation by meeting the following three requirements.

First, the trapped-ion quantum computer must be able to perform arbitrary rotations on qubits, which are already discussed in the "arbitrary single-qubit rotation" section.

The next component of a CNOT gate is the controlled phase-flip gate, or the controlled-*X* gate (see quantum logic gate). In a trapped-ion quantum computer, the state of the center of mass phonon functions as the control qubit, and the internal atomic spin state of the ion is the working qubit. The phase of the working qubit will therefore be flipped if the phonon qubit is in the state $|\mathbf{1}\rangle$.

Lastly, a SWAP gate must be implemented, acting on both the ion state and the phonon state.[1]

Two alternate schemes to represent the CNOT gates are presented in Michael Nielsen and Isaac Chuang's *Quantum Computation and Quantum Information* and Cirac and Zoller's *Quantum Computation with Cold Trapped Ions*.[1][3]

References

1. Nielsen, Michael A. (2010). *Quantum computation and quantum information*. Chuang, Isaac L., 1968– (10th anniversary ed.). Cambridge: Cambridge University Press. ISBN 9781107002173. OCLC 665137861 (https://search.worldcat.org/oclc/665137861).

2. Moses, S. A.; Baldwin, C. H.; Allman, M. S.; Ancona, R.; Ascarrunz, L.; Barnes, C.; Bartolotta, J.; Bjork, B.; Blanchard, P.; Bohn, M.; Bohnet, J. G.; Brown, N. C.; Burdick, N. Q.; Burton, W. C.; Campbell, S. L. (2023-12-18). "A Race-Track Trapped-Ion Quantum Processor" (https://link.aps.org/doi/10.1103/PhysRevX.13.041052). *Physical Review X*. **13** (4). arXiv:2305.03828 (https://arxiv.org/abs/2305.03828). doi:10.1103/PhysRevX.13.041052 (https://doi.org/10.1103%2FPhysRevX.13.041052). ISSN 2160-3308 (https://search.worldcat.org/issn/2160-3308).
3. Cirac, J. I.; Zoller, P. (1995-05-15). "Quantum Computations with Cold Trapped Ions". *Physical Review Letters*. **74** (20): 4091–4094. Bibcode:1995PhRvL..74.4091C (https://ui.adsabs.harvard.edu/abs/1995PhRvL..74.4091C). doi:10.1103/physrevlett.74.4091 (https://doi.org/10.1103%2Fphysrevlett.74.4091). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 10058410 (https://pubmed.ncbi.nlm.nih.gov/10058410).
4. Pogorelov, I.; Feldker, T.; Marciniak, Ch. D.; Postler, L.; Jacob, G.; Krieglsteiner, O.; Podlesnic, V.; Meth, M.; Negnevitsky, V.; Stadler, M.; Höfer, B.; Wächter, C.; Lakhmanskiy, K.; Blatt, R.; Schindler, P.; Monz, T. (17 June 2021). "Compact Ion-Trap Quantum Computing Demonstrator" (https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.2.020343). *PRX Quantum*. **2** (2): 020343. arXiv:2101.11390 (https://arxiv.org/abs/2101.11390). Bibcode:2021PRXQ....2b0343P (https://ui.adsabs.harvard.edu/abs/2021PRXQ....2b0343P). doi:10.1103/PRXQuantum.2.020343 (https://doi.org/10.1103%2FPRXQuantum.2.020343). S2CID 231719119 (https://api.semanticscholar.org/CorpusID:231719119). Archived (https://web.archive.org/web/20210711113855/https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.2.020343) from the original on 11 July 2021. Retrieved 11 July 2021.
5. "Quantum computer is smallest ever, claim physicists" (https://physicsworld.com/a/quantum-computer-is-smallest-ever-claim-physicists/). *Physics World*. 7 July 2021. Archived (https://web.archive.org/web/20210711113856/https://physicsworld.com/a/quantum-computer-is-smallest-ever-claim-physicists/) from the original on 11 July 2021. Retrieved 11 July 2021.
6. "The Nobel Prize in Physics 1989" (http://nobelprize.org/physics/laureates/1989/illpres/trap.html). Archived (https://web.archive.org/web/20051216150353/http://nobelprize.org/physics/laureates/1989/illpres/trap.html) from the original on 2005-12-16. Retrieved 2005-06-22.
7. "Introduction to Ion Trap Quantum Computing | University of Oxford Department of Physics" (https://www2.physics.ox.ac.uk/research/ion-trap-quantum-computing-group/intro-to-ion-trap-qc). *www2.physics.ox.ac.uk*. Archived (https://web.archive.org/web/20181112204448/https://www2.physics.ox.ac.uk/research/ion-trap-quantum-computing-group/intro-to-ion-trap-qc) from the original on 2018-11-12. Retrieved 2018-11-05.
8. Waki, I.; Kassner, S.; Birkl, G.; Walther, H. (March 30, 1992). "Observation of ordered structures of laser-cooled ions in a quadrupole storage ring" (https://link.aps.org/doi/10.1103/PhysRevLett.68.2007). *Phys. Rev. Lett*. **68** (13): 2007--2010. doi:10.1103/PhysRevLett.68.2007 (https://doi.org/10.1103%2FPhysRevLett.68.2007).
9. Raizen, M. G.; Gilligan, J. M.; Bergquist, J. C.; Itano, W. M.; Wineland, D. J. (May 1, 1992). "Ionic crystals in a linear Paul trap" (https://link.aps.org/doi/10.1103/PhysRevA.45.6493). *Phys. Rev. A*. **45** (9): 6493--6501. doi:10.1103/PhysRevA.45.6493 (https://doi.org/10.1103%2FPhysRevA.45.6493).
10. Birkl, G.; Kassner, S.; Walther, H. (May 28, 1992). "Multiple-shell structures of laser-cooled 24Mg+ ions in a quadrupole storage ring" (https://doi.org/10.1038/357310a0). *Nature*. **357** (6376): 310--313. doi:10.1038/357310a0 (https://doi.org/10.1038%2F357310a0).
11. Blinov, B; Leibfried, D; Monroe, C; Wineland, D (2004). "Quantum Computing with Trapped Ion Hyperfine Qubits". *Quantum Information Processing*. **3** (1–5): 45–59. doi:10.1007/s11128-004-9417-3 (https://doi.org/10.1007%2Fs11128-004-9417-3). hdl:2027.42/45527 (https://hdl.handle.net/2027.42%2F45527). S2CID 22586758 (https://api.semanticscholar.org/CorpusID:22586758).

12. Schindler, Philipp; Nigg, Daniel; Monz, Thomas; Barreiro, Julio T.; Martinez, Esteban; Wang, Shannon X.; Stephan Quint; Brandl, Matthias F.; Nebendahl, Volckmar (2013). "A quantum information processor with trapped ions" (http://stacks.iop.org/1367-2630/15/i=12/a=123012). *New Journal of Physics*. **15** (12): 123012. arXiv:1308.3096 (https://arxiv.org/abs/1308.3096). Bibcode:2013NJPh...15l3012S (https://ui.adsabs.harvard.edu/abs/2013NJPh...15l3012S). doi:10.1088/1367-2630/15/12/123012 (https://doi.org/10.1088%2F1367-2630%2F15%2F12%2F123012). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 55746874 (https://api.semanticscholar.org/CorpusID:55746874). Archived (https://web.archive.org/web/20211027222225/https://captcha.perfdrive.com/captcha-public/css/shieldsquare_styles.min.css) from the original on 2021-10-27. Retrieved 2018-12-04.
13. An, Fangzhao Alex; Ransford, Anthony; Schaffer, Andrew; Sletten, Lucas R.; Gaebler, John; Hostetter, James; Vittorini, Grahame (2022-09-19). "High Fidelity State Preparation and Measurement of Ion Hyperfine Qubits with $I>\frac{1}{2}$" (https://link.aps.org/doi/10.1103/PhysRevLett.129.130501). *Physical Review Letters*. **129** (13): 130501. arXiv:2203.01920 (https://arxiv.org/abs/2203.01920). doi:10.1103/PhysRevLett.129.130501 (https://doi.org/10.1103%2FPhysRevLett.129.130501). PMID 36206427 (https://pubmed.ncbi.nlm.nih.gov/36206427). S2CID 252391492 (https://api.semanticscholar.org/CorpusID:252391492).
14. Garcia-Ripoll, J.J.; Zoller, P.; Cirac, J. I. (October 7, 2003). "Fast and robust two-qubit gates for scalable ion trap quantum computing". *Physical Review Letters*. **91** (15): 157901. arXiv:quant-ph/0306006 (https://arxiv.org/abs/quant-ph/0306006). doi:10.1103/PhysRevLett.91.157901 (https://doi.org/10.1103%2FPhysRevLett.91.157901). PMID 14611499 (https://pubmed.ncbi.nlm.nih.gov/14611499). S2CID 119414046 (https://api.semanticscholar.org/CorpusID:119414046).
15. Kielpinski, D.; Monroe, C.; Wineland, D. J. (June 2002). "Architecture for a large-scale ion-trap quantum computer" (https://deepblue.lib.umich.edu/bitstream/2027.42/62880/1/nature00784.pdf) (PDF). *Nature*. **417** (6890): 709–711. Bibcode:2002Natur.417..709K (https://ui.adsabs.harvard.edu/abs/2002Natur.417..709K). doi:10.1038/nature00784 (https://doi.org/10.1038%2Fnature00784). hdl:2027.42/62880 (https://hdl.handle.net/2027.42%2F62880). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). PMID 12066177 (https://pubmed.ncbi.nlm.nih.gov/12066177). S2CID 4347109 (https://api.semanticscholar.org/CorpusID:4347109). Archived (https://web.archive.org/web/20211027222222/https://deepblue.lib.umich.edu/bitstream/handle/2027.42/62880/nature00784.pdf;jsessionid=15789D8DE13E91E909948DE272FF2887?sequence=1) from the original on 2021-10-27. Retrieved 2019-09-26.

Additional resources

- Wineland, D. J.; Monroe, C.; Itano, W. M.; Leibfried, D.; King, B. E.; Meekhof, D. M. (1998). "Experimental Issues in Coherent Quantum-State Manipulation of Trapped Atomic Ions" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4898965). *Journal of Research of the National Institute of Standards and Technology*. **103** (3): 259–328. arXiv:quant-ph/9710025 (https://arxiv.org/abs/quant-ph/9710025). doi:10.6028/jres.103.019 (https://doi.org/10.6028%2Fjres.103.019). PMC 4898965 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4898965). PMID 28009379 (https://pubmed.ncbi.nlm.nih.gov/28009379).
- Leibfried, D; Blatt, R; Monroe, C; Wineland, D (2003). "Quantum dynamics of single trapped ions". *Reviews of Modern Physics*. **75** (1): 281–324. Bibcode:2003RvMP...75..281L (https://ui.adsabs.harvard.edu/abs/2003RvMP...75..281L). doi:10.1103/revmodphys.75.281 (https://doi.org/10.1103%2Frevmodphys.75.281).
- Steane, A. (1997). "The ion trap quantum information processor". *Appl. Phys. B*. **64** (6): 623–643. arXiv:quant-ph/9608011 (https://arxiv.org/abs/quant-ph/9608011). Bibcode:1996ApPhB..64..623S (https://ui.adsabs.harvard.edu/abs/1996ApPhB..64..623S). doi:10.1007/s003400050225 (https://doi.org/10.1007%2Fs003400050225). S2CID 2061791 (https://api.semanticscholar.org/CorpusID:2061791).

- Monroe, C.; et al. (1995). "Demonstration of a Fundamental Quantum Logic Gate" (https://doi.org/10.1103%2Fphysrevlett.75.4714). *Phys. Rev. Lett*. **75** (25): 4714–4717. Bibcode:1995PhRvL..75.4714M (https://ui.adsabs.harvard.edu/abs/1995PhRvL..75.4714M). doi:10.1103/physrevlett.75.4714 (https://doi.org/10.1103%2Fphysrevlett.75.4714). PMID 10059979 (https://pubmed.ncbi.nlm.nih.gov/10059979).
- Trapped ion computer on arxiv.org (http://xstructure.inr.ac.ru/x-bin/theme3.py?level=2&index1=-134326)
- Friedenauer, A.; Schmitz, H.; Glueckert, J. T.; Porras, D.; Schaetz, T. (2008). "Simulating a quantum magnet with trapped ions" (https://doi.org/10.1038%2Fnphys1032). *Nature Physics*. **4** (10): 757–761. Bibcode:2008NatPh...4..757F (https://ui.adsabs.harvard.edu/abs/2008NatPh...4..757F). doi:10.1038/nphys1032 (https://doi.org/10.1038%2Fnphys1032).
- Moehring, D. L.; Maunz, P.; Olmschenk, S.; Younge, K. C.; Matsukevich, D. N.; Duan, L.-M.; Monroe, C. (2007). "Entanglement of single-atom quantum bits at a distance". *Nature*. **449** (7158): 68–71. Bibcode:2007Natur.449...68M (https://ui.adsabs.harvard.edu/abs/2007Natur.449...68M). doi:10.1038/nature06118 (https://doi.org/10.1038%2Fnature06118). hdl:2027.42/62780 (https://hdl.handle.net/2027.42%2F62780). PMID 17805290 (https://pubmed.ncbi.nlm.nih.gov/17805290). S2CID 19624141 (https://api.semanticscholar.org/CorpusID:19624141).
- Stick, D.; Hensinger, W. K.; Olmschenk, S.; Madsen, M. J.; Schwab, K.; Monroe, C. (2006). "Ion trap in a semiconductor chip". *Nature Physics*. **2** (1): 36–39. arXiv:quant-ph/0601052 (https://arxiv.org/abs/quant-ph/0601052). Bibcode:2006NatPh...2...36S (https://ui.adsabs.harvard.edu/abs/2006NatPh...2...36S). doi:10.1038/nphys171 (https://doi.org/10.1038%2Fnphys171). S2CID 5419269 (https://api.semanticscholar.org/CorpusID:5419269).
- Leibfried, D.; Knill, E.; Seidelin, S.; Britton, J.; Blakestad, R. B.; Chiaverini, J.; Hume, D. B.; Itano, W. M.; Jost, J. D.; Langer, C.; Ozeri, R.; Reichle, R.; Wineland, D. J. (2005). "Creation of a six-atom 'Schrödinger cat' state". *Nature*. **438** (7068): 639–642. Bibcode:2005Natur.438..639L (https://ui.adsabs.harvard.edu/abs/2005Natur.438..639L). doi:10.1038/nature04251 (https://doi.org/10.1038%2Fnature04251). PMID 16319885 (https://pubmed.ncbi.nlm.nih.gov/16319885). S2CID 4370887 (https://api.semanticscholar.org/CorpusID:4370887).
- Häffner, H.; Hänsel, W.; Roos, C. F.; Benhelm, J.; Chek-al-kar, D.; Chwalla, M.; Körber, T.; Rapol, U. D.; Riebe, M.; Schmidt, P. O.; Becher, C.; Gühne, O.; Dür, W.; Blatt, R. (2005). "Scalable multiparticle entanglement of trapped ions". *Nature*. **438** (7068): 643–646. arXiv:quant-ph/0603217 (https://arxiv.org/abs/quant-ph/0603217). Bibcode:2005Natur.438..643H (https://ui.adsabs.harvard.edu/abs/2005Natur.438..643H). doi:10.1038/nature04279 (https://doi.org/10.1038%2Fnature04279). PMID 16319886 (https://pubmed.ncbi.nlm.nih.gov/16319886). S2CID 4411480 (https://api.semanticscholar.org/CorpusID:4411480).
- Chiaverini, J.; Britton, J.; Leibfried, D.; Knill, E.; Barrett, M. D.; Blakestad, R. B.; Itano, W.M.; Jost, J.D.; Langer, C.; Ozeri, R.; Schaetz, T.; Wineland, D.J. (2005). "Implementation of the semiclassical quantum Fourier transform in a scalable system". *Science*. **308** (5724): 997–1000. Bibcode:2005Sci...308..997C (https://ui.adsabs.harvard.edu/abs/2005Sci...308..997C). doi:10.1126/science.1110335 (https://doi.org/10.1126%2Fscience.1110335). PMID 15890877 (https://pubmed.ncbi.nlm.nih.gov/15890877). S2CID 15550997 (https://api.semanticscholar.org/CorpusID:15550997).
- Blinov, B. B.; Moehring, D. L.; Duan, L.- M.; Monroe, C. (2004). "Observation of entanglement between a single trapped atom and a single photon" (https://deepblue.lib.umich.edu/bitstream/2027.42/62924/1/nature02377.pdf) (PDF). *Nature*. **428** (6979): 153–157. Bibcode:2004Natur.428..153B (https://ui.adsabs.harvard.edu/abs/2004Natur.428..153B). doi:10.1038/nature02377 (https://doi.org/10.1038%2Fnature02377). hdl:2027.42/62924 (https://hdl.handle.net/2027.42%2F62924). PMID 15014494 (https://pubmed.ncbi.nlm.nih.gov/15014494). S2CID 4314514 (https://api.semanticscholar.org/CorpusID:4314514).

- Chiaverini, J.; Leibried, D.; Schaetz, T.; Barrett, M. D.; Blakestad, R. B.; Britton, J.; Itano, W.M.; Jost, J.D.; Knill, E.; Langer, C.; Ozeri, R.; Wineland, D.J. (2004). "Realization of quantum error correction". *Nature*. **432** (7017): 602–605. Bibcode:2004Natur.432..602C (https://ui.adsabs.harvard.edu/abs/2004Natur.432..602C). doi:10.1038/nature03074 (https://doi.org/10.1038%2Fnature03074). PMID 15577904 (https://pubmed.ncbi.nlm.nih.gov/15577904). S2CID 167898 (https://api.semanticscholar.org/CorpusID:167898).
- Riebe, M.; Häffner, H.; Roos, C. F.; Hänsel, W.; Benhelm, J.; Lancaster, G. P. T.; Körber, T. W.; Becher, C.; Schmidt-Kaler, F.; James, D. F. V.; Blatt, R. (2004). "Deterministic quantum teleportation with atoms". *Nature*. **429** (6993): 734–737. Bibcode:2004Natur.429..734R (https://ui.adsabs.harvard.edu/abs/2004Natur.429..734R). doi:10.1038/nature02570 (https://doi.org/10.1038%2Fnature02570). PMID 15201903 (https://pubmed.ncbi.nlm.nih.gov/15201903). S2CID 4397716 (https://api.semanticscholar.org/CorpusID:4397716).
- Barrett, M. D.; Chiaverini, J.; Schaetz, T.; Britton, J.; Itano, W.M.; Jost, J.D.; Knill, E.; Langer, C.; Leibfried, D.; Ozeri, R.; Wineland, D.J. (2004). "Deterministic quantum teleportation of atomic qubits". *Nature*. **429** (6993): 737–739. Bibcode:2004Natur.429..737B (https://ui.adsabs.harvard.edu/abs/2004Natur.429..737B). doi:10.1038/nature02608 (https://doi.org/10.1038%2Fnature02608). PMID 15201904 (https://pubmed.ncbi.nlm.nih.gov/15201904). S2CID 1608775 (https://api.semanticscholar.org/CorpusID:1608775).
- Roos, C. F.; Riebe, M.; Häffner, H.; Hänsel, W.; Benhelm, J.; Lancaster, G. P. T.; Becher, C.; Schmidt-Kaler, F.; Blatt, R. (2004). "Control and measurement of three-qubit entangled state". *Science*. **304** (5676): 1478–1480. Bibcode:2004Sci...304.1478R (https://ui.adsabs.harvard.edu/abs/2004Sci...304.1478R). doi:10.1126/science.1097522 (https://doi.org/10.1126%2Fscience.1097522). PMID 15178795 (https://pubmed.ncbi.nlm.nih.gov/15178795). S2CID 12020439 (https://api.semanticscholar.org/CorpusID:12020439).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Trapped-ion_quantum_computer&oldid=1233477696"

-

WIKIPEDIA
The Free Encyclopedia

Spin (physics)

Spin is an intrinsic form of angular momentum carried by elementary particles, and thus by composite particles such as hadrons, atomic nuclei, and atoms.[1][2]:183 (https://archive.org/details/introductiontoqu00grif_190/page/n194)–184 Spin is quantized, and accurate models for the interaction with spin require relativistic quantum mechanics or quantum field theory.

The existence of electron spin angular momentum is inferred from experiments, such as the Stern–Gerlach experiment, in which silver atoms were observed to possess two possible discrete angular momenta despite having no orbital angular momentum.[3] The relativistic spin–statistics theorem connects electron spin quantization to the Pauli exclusion principle: observations of exclusion imply spin and observations of spin imply exclusion.

Spin is described mathematically as a vector for some particles such as photons, and as spinors and bispinors for other particles such as electrons. Spinors and bispinors behave similarly to vectors: they have definite magnitudes and change under rotations; however, they use an unconventional "direction". All elementary particles of a given kind have the same magnitude of spin angular momentum, though its direction may change. These are indicated by assigning the particle a spin quantum number.[2]:183–184 (https://archive.org/details/introductiontoqu00grif_190/page/n194)

The SI units of spin are the same as classical angular momentum (i.e., N·m·s, J·s, or $kg \cdot m^2 \cdot s^{-1}$). In quantum mechanics, angular momentum and spin angular momentum take discrete values proportional to the Planck constant. In practice, spin is usually given as a dimensionless spin quantum number by dividing the spin angular momentum by the reduced Planck constant $\hbar$. Often, the "spin quantum number" is simply called "spin".

Models

Rotating charged mass

The earliest models for electron spin imagined a rotating charged mass, but this model fails when examined in detail: the required space distribution does not match limits on the electron radius: the required rotation speed exceeds the speed of light.[4] In the Standard Model, the fundamental particles are all considered "point-like": they have their effects through the field that surrounds them.[5] Any model for spin based on mass rotation would need to be consistent with that model.

Pauli's "classically non-describable two-valuedness"

Wolfgang Pauli, a central figure in the history of quantum spin, initially rejected any idea that the "degree of freedom" he introduced to explain experimental observations was related to rotation. He called it "classically non-describable two-valuedness". Later he allowed that it is related to angular momentum, but insisted on considering spin an abstract property.[6] This approach allowed Pauli to develop a proof of his fundamental Pauli exclusion principle, a proof now called the spin-statistics theorem.[7] In retrospect this insistence and the style of his proof initiated the modern particle physics era, where abstract quantum properties derived from symmetry properties dominate. Concrete interpretation became secondary and optional.[6]

Circulation of classical fields

The first classical model for spin proposed small rigid particle rotating about an axis, as ordinary use of the word may suggest. Angular momentum can be computed from a classical field as well.[8][9]:63 By applying Frederik Belinfante's approach to calculating the angular momentum of a field, Hans C. Ohanian showed that "spin is essentially a wave property ... generated by a circulating flow of charge in the wave field of the electron".[10] This same concept of spin can be applied to gravity waves in water: "spin is generated by subwavelength circular motion of water particles".[11]

Unlike classical wavefield circulation which allows continuous values of angular momentum, quantum wavefields allow only discrete values.[10] Consequently energy transfer to or from spins states always occurs in fixed quantum steps. Only a few steps are allowed: for many qualitative purposes the complexity of the spin quantum wavefields can be ignored and the system properties can be discussed in terms of "integer" or "half-integer" spin models as discussed in quantum numbers below.

Dirac's relativistic electron

Quantitative calculations of spin properties for electrons requires the Dirac's relativistic wave equation.[7]

Relation to orbital angular momentum

As the name suggests, spin was originally conceived as the rotation of a particle around some axis. Historically orbital angular momentum related to particle orbits.[12]:131 While the names based on mechanical models have survived, the physical explanation has not. Quantization fundamentally alters the character of both spin and orbital angular momentum.

Since elementary particles are point-like, self-rotation is not well-defined for them. However, spin implies that the phase of the particle depends on the angle as $e^{iS\theta}$, for rotation of angle θ around the axis parallel to the spin S. This is equivalent to the quantum-mechanical interpretation of momentum as phase dependence in the position, and of orbital angular momentum as phase dependence in the angular position.

For fermions, the picture is less clear. Angular velocity is equal by the Ehrenfest theorem to the derivative of the Hamiltonian to its conjugate momentum, which is the total angular momentum operator $\mathbf{J} = \mathbf{L} + \mathbf{S}$. Therefore, if the Hamiltonian H is dependent upon the spin S, dH/dS is non-zero, and the spin causes angular velocity, and hence actual rotation, i.e. a change in the phase-angle relation over time. However, whether this holds for free electron is ambiguous, since

for an electron, S^2 is constant, and therefore it is a matter of interpretation whether the Hamiltonian includes such a term. Nevertheless, spin appears in the Dirac equation, and thus the relativistic Hamiltonian of the electron, treated as a Dirac field, can be interpreted as including a dependence in the spin S.[9]

Quantum number

Spin obeys the mathematical laws of angular momentum quantization. The specific properties of spin angular momenta include:

- Spin quantum numbers may take either half-integer or integer values.
- Although the direction of its spin can be changed, the magnitude of the spin of an elementary particle cannot be changed.
- The spin of a charged particle is associated with a magnetic dipole moment with a g-factor that differs from 1. (In the classical context, this would imply the internal charge and mass distributions differing for a rotating object.[4])

The conventional definition of the **spin quantum number** is $s = \frac{n}{2}$, where n can be any non-negative integer. Hence the allowed values of s are 0, $\frac{1}{2}$, 1, $\frac{3}{2}$, 2, etc. The value of s for an elementary particle depends only on the type of particle and cannot be altered in any known way (in contrast to the *spin direction* described below). The spin angular momentum S of any physical system is quantized. The allowed values of S are

$$S = \hbar\sqrt{s(s+1)} = \frac{h}{2\pi}\sqrt{\frac{n}{2}\frac{(n+2)}{2}} = \frac{h}{4\pi}\sqrt{n(n+2)},$$

where h is the Planck constant, and $\hbar = \frac{h}{2\pi}$ is the reduced Planck constant. In contrast, orbital angular momentum can only take on integer values of s; i.e., even-numbered values of n.

Fermions and bosons

Those particles with half-integer spins, such as $\frac{1}{2}$, $\frac{3}{2}$, $\frac{5}{2}$, are known as fermions, while those particles with integer spins, such as 0, 1, 2, are known as bosons. The two families of particles obey different rules and *broadly* have different roles in the world around us. A key distinction between the two families is that fermions obey the Pauli exclusion principle: that is, there cannot be two identical fermions simultaneously having the same quantum numbers (meaning, roughly, having the same position, velocity and spin direction). Fermions obey the rules of Fermi–Dirac statistics. In contrast, bosons obey the rules of Bose–Einstein statistics and have no such restriction, so they may "bunch together" in identical states. Also, composite particles can have spins different from their component particles. For example, a helium-4 atom in the ground state has spin 0 and behaves like a boson, even though the quarks and electrons which make it up are all fermions.

This has some profound consequences:

- Quarks and leptons (including electrons and neutrinos), which make up what is classically known as matter, are all fermions with spin $\frac{1}{2}$. The common idea that "matter takes up space" actually comes from the Pauli exclusion principle acting on these particles to prevent the fermions from being in the same quantum state. Further compaction would require electrons to occupy the same energy states, and therefore a kind of pressure (sometimes known as degeneracy pressure of electrons) acts to resist the fermions being overly close.

  Elementary fermions with other spins ($\frac{3}{2}$, $\frac{5}{2}$, etc.) are not known to exist.
- Elementary particles which are thought of as carrying forces are all bosons with spin 1. They include the photon, which carries the electromagnetic force, the gluon (strong force), and the W and Z bosons (weak force). The ability of bosons to occupy the same quantum state is used in the laser, which aligns many photons having the same quantum number (the same direction and frequency), superfluid liquid helium resulting from helium-4 atoms being bosons, and superconductivity, where pairs of electrons (which individually are fermions) act as single composite bosons.

  Elementary bosons with other spins (0, 2, 3, etc.) were not historically known to exist, although they have received considerable theoretical treatment and are well established within their respective mainstream theories. In particular, theoreticians have proposed the graviton (predicted to exist by some quantum gravity theories) with spin 2, and the Higgs boson (explaining electroweak symmetry breaking) with spin 0. Since 2013, the Higgs boson with spin 0 has been considered proven to exist.[13] It is the first scalar elementary particle (spin 0) known to exist in nature.
- Atomic nuclei have nuclear spin which may be either half-integer or integer, so that the nuclei may be either fermions or bosons.

Spin–statistics theorem

The spin–statistics theorem splits particles into two groups: bosons and fermions, where bosons obey Bose–Einstein statistics, and fermions obey Fermi–Dirac statistics (and therefore the Pauli exclusion principle). Specifically, the theorem requires that particles with half-integer spins obey the Pauli exclusion principle while particles with integer spin do not. As an example, electrons have half-integer spin and are fermions that obey the Pauli exclusion principle, while photons have integer spin and do not. The theorem was derived by Wolfgang Pauli in 1940; it relies on both quantum mechanics and the theory of special relativity. Pauli described this connection between spin and statistics as "one of the most important applications of the special relativity theory".[14]

Magnetic moments

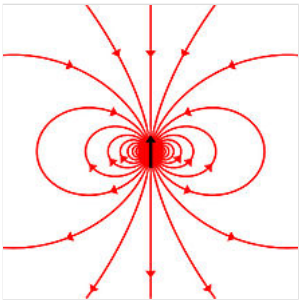
Particles with spin can possess a magnetic dipole moment, just like a rotating electrically charged body in classical electrodynamics. These magnetic moments can be experimentally observed in several ways, e.g. by the deflection of particles by inhomogeneous magnetic fields in a Stern–Gerlach experiment, or by measuring the magnetic fields generated by the particles themselves.

The intrinsic magnetic moment $\boldsymbol{\mu}$ of a spin-$\frac{1}{2}$ particle with charge q, mass m, and spin angular momentum $\mathbf{S}$, is[15]

$$\boldsymbol{\mu} = \frac{g_s q}{2m}\mathbf{S},$$

where the dimensionless quantity g_s is called the spin g-factor. For exclusively orbital rotations it would be 1 (assuming that the mass and the charge occupy spheres of equal radius).

The electron, being a charged elementary particle, possesses a nonzero magnetic moment. One of the triumphs of the theory of quantum electrodynamics is its accurate prediction of the electron g-factor, which has been experimentally determined to have the value −2.002 319 304 360 92(36), with the digits in parentheses denoting measurement uncertainty in the last two digits at one standard deviation.[16] The value of 2 arises from the Dirac equation, a fundamental equation connecting the electron's spin with its electromagnetic properties, and the deviation from −2 arises from the electron's interaction with the surrounding quantum fields, including its own electromagnetic field and virtual particles.[17]



Schematic diagram depicting the spin of the neutron as the black arrow and magnetic field lines associated with the neutron magnetic moment. The neutron has a negative magnetic moment. While the spin of the neutron is upward in this diagram, the magnetic field lines at the center of the dipole are downward.

Composite particles also possess magnetic moments associated with their spin. In particular, the neutron possesses a non-zero magnetic moment despite being electrically neutral. This fact was an early indication that the neutron is not an elementary particle. In fact, it is made up of quarks, which are electrically charged particles. The magnetic moment of the neutron comes from the spins of the individual quarks and their orbital motions.

Neutrinos are both elementary and electrically neutral. The minimally extended Standard Model that takes into account non-zero neutrino masses predicts neutrino magnetic moments of:[18][19][20]

$$\mu_\nu \approx 3 \times 10^{-19} \mu_\mathrm{B} \frac{m_\nu c^2}{\mathrm{eV}},$$

where the μ_ν are the neutrino magnetic moments, m_ν are the neutrino masses, and μ_B is the Bohr magneton. New physics above the electroweak scale could, however, lead to significantly higher neutrino magnetic moments. It can be shown in a model-independent way that neutrino magnetic moments larger than about $10^{-14}\,\mu_\mathrm{B}$ are "unnatural" because they would also lead to large radiative contributions to the neutrino mass. Since the neutrino masses are known to be at most about 1 eV/c^2, fine-tuning would be necessary in order to prevent large contributions to the neutrino mass via radiative corrections.[21] The measurement of neutrino magnetic moments is an active area of research. Experimental results have put the neutrino magnetic moment at less than 1.2×10^{-10} times the electron's magnetic moment.

On the other hand elementary particles with spin but without electric charge, such as a photon or a Z boson, do not have a magnetic moment.

Curie temperature and loss of alignment

In ordinary materials, the magnetic dipole moments of individual atoms produce magnetic fields that cancel one another, because each dipole points in a random direction, with the overall average being very near zero. Ferromagnetic materials below their Curie temperature, however, exhibit magnetic domains in which the atomic dipole moments spontaneously align locally, producing a macroscopic, non-zero magnetic field from the domain. These are the ordinary "magnets" with which we are all familiar.

In paramagnetic materials, the magnetic dipole moments of individual atoms will partially align with an externally applied magnetic field. In diamagnetic materials, on the other hand, the magnetic dipole moments of individual atoms align oppositely to any externally applied magnetic field, even if it requires energy to do so.

The study of the behavior of such "spin models" is a thriving area of research in condensed matter physics. For instance, the Ising model describes spins (dipoles) that have only two possible states, up and down, whereas in the Heisenberg model the spin vector is allowed to point in any direction. These models have many interesting properties, which have led to interesting results in the theory of phase transitions.

Direction

Spin projection quantum number and multiplicity

In classical mechanics, the angular momentum of a particle possesses not only a magnitude (how fast the body is rotating), but also a direction (either up or down on the axis of rotation of the particle). Quantum-mechanical spin also contains information about direction, but in a more subtle form. Quantum mechanics states that the component of angular momentum for a spin-s particle measured along any direction can only take on the values[22]

$$S_i = \hbar s_i, \quad s_i \in \{-s, -(s-1), \dots, s-1, s\},$$

where S_i is the spin component along the i-th axis (either x, y, or z), s_i is the spin projection quantum number along the i-th axis, and s is the principal spin quantum number (discussed in the previous section). Conventionally the direction chosen is the z axis:

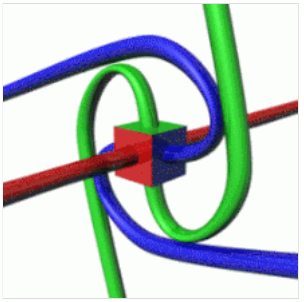
$$S_z = \hbar s_z, \quad s_z \in \{-s, -(s-1), \dots, s-1, s\},$$

where S_z is the spin component along the z axis, s_z is the spin projection quantum number along the z axis.

One can see that there are $2s + 1$ possible values of s_z. The number "$2s + 1$" is the multiplicity of the spin system. For example, there are only two possible values for a spin-$\frac{1}{2}$ particle: $s_z = +\frac{1}{2}$ and $s_z = -\frac{1}{2}$. These correspond to quantum states in which the spin component is pointing in the $+z$ or $-z$ directions respectively, and are often referred to as "spin up" and "spin down". For a spin-$\frac{3}{2}$ particle, like a delta baryon, the possible values are $+\frac{3}{2}$, $+\frac{1}{2}$, $-\frac{1}{2}$, $-\frac{3}{2}$.

Vector

For a given quantum state, one could think of a spin vector $\langle \boldsymbol{S} \rangle$ whose components are the expectation values of the spin components along each axis, i.e., $\langle \boldsymbol{S} \rangle = [\langle \boldsymbol{S}_x \rangle, \langle \boldsymbol{S}_y \rangle, \langle \boldsymbol{S}_z \rangle]$. This vector then would describe the "direction" in which the spin is pointing, corresponding to the classical concept of the axis of rotation. It turns out that the spin vector is not very useful in actual quantum-mechanical calculations, because it cannot be measured directly: s_x, s_y and s_z cannot possess simultaneous definite values, because of a quantum uncertainty relation between them. However, for statistically large collections of particles that have been placed in the same pure quantum state, such as through the use of a Stern–Gerlach apparatus, the spin vector does have a well-defined experimental meaning: It specifies the direction in ordinary space in which a subsequent detector must be oriented in order to achieve the maximum possible probability (100%) of detecting every particle in the collection. For spin-$\frac{1}{2}$ particles, this probability drops off smoothly as the angle between the spin vector and the detector increases, until at an angle of 180°—that is, for detectors oriented in the opposite direction to the spin vector—the expectation of detecting particles from the collection reaches a minimum of 0%.



A single point in space can rotate continuously without becoming tangled. Notice that after a 360-degree rotation, the spiral flips between clockwise and counterclockwise orientations. It returns to its original configuration after spinning a full 720°.

As a qualitative concept, the spin vector is often handy because it is easy to picture classically. For instance, quantum-mechanical spin can exhibit phenomena analogous to classical gyroscopic effects. For example, one can exert a kind of "torque" on an electron by putting it in a magnetic field (the field acts upon the electron's intrinsic magnetic dipole moment—see the following section). The result is that the spin vector undergoes precession, just like a classical gyroscope. This phenomenon is known as electron spin resonance (ESR). The equivalent behaviour of protons in atomic nuclei is used in nuclear magnetic resonance (NMR) spectroscopy and imaging.

Mathematically, quantum-mechanical spin states are described by vector-like objects known as spinors. There are subtle differences between the behavior of spinors and vectors under coordinate rotations. For example, rotating a spin-$\frac{1}{2}$ particle by 360° does not bring it back to the same quantum state, but to the state with the opposite quantum phase; this is detectable, in principle, with interference experiments. To return the particle to its exact original state, one needs a 720° rotation. (The plate trick and Möbius strip give non-quantum analogies.) A spin-zero particle can only have a single quantum state, even after torque is applied. Rotating a spin-2 particle 180° can bring it back to the same quantum state, and a spin-4 particle should be rotated 90° to bring it back to the same quantum state. The spin-2 particle can be analogous to a straight stick that looks the same even after it is rotated 180°, and a spin-0 particle can be imagined as sphere, which looks the same after whatever angle it is turned through.

Mathematical formulation

Operator

Spin obeys commutation relations[23] analogous to those of the orbital angular momentum:

$$\left[\hat{\boldsymbol{S}}_j, \hat{\boldsymbol{S}}_k\right] = i\hbar\varepsilon_{jkl}\hat{\boldsymbol{S}}_l,$$

where ε_{jkl} is the Levi-Civita symbol. It follows (as with angular momentum) that the eigenvectors of $\hat{\boldsymbol{S}}^2$ and $\hat{\boldsymbol{S}}_z$ (expressed as kets in the total S basis) are[2]:166

$$\hat{\boldsymbol{S}}^2|s, m_s\rangle = \hbar^2 s(s+1)|s, m_s\rangle,$$
$$\hat{\boldsymbol{S}}_z|s, m_s\rangle = \hbar m_s|s, m_s\rangle.$$

The spin raising and lowering operators acting on these eigenvectors give

$$\hat{\boldsymbol{S}}_\pm|s, m_s\rangle = \hbar\sqrt{s(s+1) - m_s(m_s \pm 1)}|s, m_s \pm 1\rangle,$$

where $\hat{\boldsymbol{S}}_\pm = \hat{\boldsymbol{S}}_x \pm i\hat{\boldsymbol{S}}_y$.[2]:166

But unlike orbital angular momentum, the eigenvectors are not spherical harmonics. They are not functions of θ and φ. There is also no reason to exclude half-integer values of s and m_s.

All quantum-mechanical particles possess an intrinsic spin $\boldsymbol{s}$ (though this value may be equal to zero). The projection of the spin $\boldsymbol{s}$ on any axis is quantized in units of the reduced Planck constant, such that the state function of the particle is, say, not $\boldsymbol{\psi} = \boldsymbol{\psi}(\mathbf{r})$, but $\boldsymbol{\psi} = \boldsymbol{\psi}(\mathbf{r}, \boldsymbol{s}_z)$, where $\boldsymbol{s}_z$ can take only the values of the following discrete set:

$$\boldsymbol{s}_z \in \{-s\hbar, -(s-1)\hbar, \ldots, +(s-1)\hbar, +s\hbar\}.$$

One distinguishes bosons (integer spin) and fermions (half-integer spin). The total angular momentum conserved in interaction processes is then the sum of the orbital angular momentum and the spin.

Pauli matrices

The quantum-mechanical operators associated with spin-$\frac{1}{2}$ observables are

$$\hat{\mathbf{S}} = \frac{\hbar}{2}\boldsymbol{\sigma},$$

where in Cartesian components

$$S_x = \frac{\hbar}{2}\sigma_x, \quad S_y = \frac{\hbar}{2}\sigma_y, \quad S_z = \frac{\hbar}{2}\sigma_z.$$

For the special case of spin-$\frac{1}{2}$ particles, σ_x, σ_y and σ_z are the three Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Pauli exclusion principle

The Pauli exclusion principle states that the wavefunction $\psi(\mathbf{r}_1, \sigma_1, \ldots, \mathbf{r}_N, \sigma_N)$ for a system of N identical particles having spin s must change upon interchanges of any two of the N particles as

$$\psi(\ldots, \mathbf{r}_i, \sigma_i, \ldots, \mathbf{r}_j, \sigma_j, \ldots) = (-1)^{2s}\psi(\ldots, \mathbf{r}_j, \sigma_j, \ldots, \mathbf{r}_i, \sigma_i, \ldots).$$

Thus, for bosons the prefactor $(-1)^{2s}$ will reduce to +1, for fermions to −1. This permutation postulate for N-particle state functions has most important consequences in daily life, e.g. the periodic table of the chemical elements.

Rotations

As described above, quantum mechanics states that components of angular momentum measured along any direction can only take a number of discrete values. The most convenient quantum-mechanical description of particle's spin is therefore with a set of complex numbers corresponding to amplitudes of finding a given value of projection of its intrinsic angular momentum on a given axis. For instance, for a spin-$\frac{1}{2}$ particle, we would need two numbers $a_{\pm 1/2}$, giving amplitudes of finding it with projection of angular momentum equal to $+\frac{\hbar}{2}$ and $-\frac{\hbar}{2}$, satisfying the requirement

$$|a_{+1/2}|^2 + |a_{-1/2}|^2 = 1.$$

For a generic particle with spin s, we would need $2s + 1$ such parameters. Since these numbers depend on the choice of the axis, they transform into each other non-trivially when this axis is rotated. It is clear that the transformation law must be linear, so we can represent it by associating a matrix with each rotation, and the product of two transformation matrices corresponding to rotations A and B must be equal (up to phase) to the matrix representing rotation AB. Further, rotations preserve the quantum-mechanical inner product, and so should our transformation matrices:

$$\sum_{m=-j}^{j} a_m^* b_m = \sum_{m=-j}^{j} \left(\sum_{n=-j}^{j} U_{nm} a_n \right)^* \left(\sum_{k=-j}^{j} U_{km} b_k \right),$$

$$\sum_{n=-j}^{j} \sum_{k=-j}^{j} U_{np}^* U_{kq} = \delta_{pq}.$$

Mathematically speaking, these matrices furnish a unitary projective representation of the rotation group SO(3). Each such representation corresponds to a representation of the covering group of SO(3), which is SU(2).[24] There is one n-dimensional irreducible representation of SU(2) for each dimension, though this representation is n-dimensional real for odd n and n-dimensional complex for even n (hence of real dimension $2n$). For a rotation by angle θ in the plane with normal vector $\hat{\boldsymbol{\theta}}$,

$$U = e^{-\frac{i}{\hbar}\boldsymbol{\theta}\cdot\mathbf{S}},$$

where $\boldsymbol{\theta} = \theta\hat{\boldsymbol{\theta}}$, and $\mathbf{S}$ is the vector of spin operators.

Proof

Working in the coordinate system where $\hat{\boldsymbol{\theta}} = \hat{\boldsymbol{z}}$, we would like to show that S_x and S_y are rotated into each other by the angle θ. Starting with S_x. Using units where $\hbar = 1$:

$$\begin{aligned} S_x \to U^\dagger S_x U &= e^{i\theta S_z} S_x e^{-i\theta S_z} \\ &= S_x + (i\theta)\,[S_z, S_x] + \left(\frac{1}{2!}\right)(i\theta)^2\,[S_z, [S_z, S_x]] + \left(\frac{1}{3!}\right)(i\theta)^3\,[S_z, [S_z, [S_z, S_x]]] + \cdots \end{aligned}$$

Using the spin operator commutation relations, we see that the commutators evaluate to $i\,S_y$ for the odd terms in the series, and to S_x for all of the even terms. Thus:

$$\begin{aligned} U^\dagger S_x U &= S_x \left[1 - \frac{\theta^2}{2!} + \cdots\right] - S_y \left[\theta - \frac{\theta^3}{3!} \cdots\right] \\ &= S_x \cos\theta - S_y \sin\theta, \end{aligned}$$

as expected. Note that since we only relied on the spin operator commutation relations, this proof holds for any dimension (i.e., for any principal spin quantum number s).[25]:164

A generic rotation in 3-dimensional space can be built by compounding operators of this type using Euler angles:

$$\mathcal{R}(\alpha, \beta, \gamma) = e^{-i\alpha S_x} e^{-i\beta S_y} e^{-i\gamma S_z}.$$

An irreducible representation of this group of operators is furnished by the Wigner D-matrix:

$$D^s_{m'm}(\alpha, \beta, \gamma) \equiv \langle sm' | \mathcal{R}(\alpha, \beta, \gamma) | sm \rangle = e^{-im'\alpha} d^s_{m'm}(\beta) e^{-im\gamma},$$

where

$$d^s_{m'm}(\beta) = \langle sm' | e^{-i\beta s_y} | sm \rangle$$

is Wigner's small d-matrix. Note that for $\gamma = 2\pi$ and $\alpha = \beta = 0$; i.e., a full rotation about the z axis, the Wigner D-matrix elements become

$$D^s_{m'm}(0, 0, 2\pi) = d^s_{m'm}(0) e^{-im2\pi} = \delta_{m'm}(-1)^{2m}.$$

Recalling that a generic spin state can be written as a superposition of states with definite m, we see that if s is an integer, the values of m are all integers, and this matrix corresponds to the identity operator. However, if s is a half-integer, the values of m are also all half-integers, giving $(-1)^{2m} = -1$ for all m, and hence upon rotation by 2π the state picks up a minus sign. This fact is a crucial element of the proof of the spin–statistics theorem.

Lorentz transformations

We could try the same approach to determine the behavior of spin under general Lorentz transformations, but we would immediately discover a major obstacle. Unlike SO(3), the group of Lorentz transformations SO(3,1) is non-compact and therefore does not have any faithful, unitary, finite-dimensional representations.

In case of spin-$\frac{1}{2}$ particles, it is possible to find a construction that includes both a finite-dimensional representation and a scalar product that is preserved by this representation. We associate a 4-component Dirac spinor ψ with each particle. These spinors transform under Lorentz transformations according to the law

$$\psi' = \exp\left(\tfrac{1}{8}\omega_{\mu\nu}[\gamma_\mu, \gamma_\nu]\right)\psi,$$

where γ_ν are gamma matrices, and $\omega_{\mu\nu}$ is an antisymmetric 4 × 4 matrix parametrizing the transformation. It can be shown that the scalar product

$$\langle \psi | \phi \rangle = \bar{\psi}\phi = \psi^\dagger \gamma_0 \phi$$

is preserved. It is not, however, positive-definite, so the representation is not unitary.

Measurement of spin along the x, y, or z axes

Each of the (Hermitian) Pauli matrices of spin-$\frac{1}{2}$ particles has two eigenvalues, +1 and −1. The corresponding normalized eigenvectors are

$$\begin{aligned}
\psi_{x+} &= \left|\tfrac{1}{2}, \tfrac{+1}{2}\right\rangle_x = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad \psi_{x-} = \left|\tfrac{1}{2}, \tfrac{-1}{2}\right\rangle_x = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, \\
\psi_{y+} &= \left|\tfrac{1}{2}, \tfrac{+1}{2}\right\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \quad \psi_{y-} = \left|\tfrac{1}{2}, \tfrac{-1}{2}\right\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}, \\
\psi_{z+} &= \left|\tfrac{1}{2}, \tfrac{+1}{2}\right\rangle_z = \begin{pmatrix}1\\0\end{pmatrix}, \quad \psi_{z-} = \left|\tfrac{1}{2}, \tfrac{-1}{2}\right\rangle_z = \begin{pmatrix}0\\1\end{pmatrix}.
\end{aligned}$$

(Because any eigenvector multiplied by a constant is still an eigenvector, there is ambiguity about the overall sign. In this article, the convention is chosen to make the first element imaginary and negative if there is a sign ambiguity. The present convention is used by software such as SymPy; while many physics textbooks, such as Sakurai and Griffiths, prefer to make it real and positive.)

By the postulates of quantum mechanics, an experiment designed to measure the electron spin on the x, y, or z axis can only yield an eigenvalue of the corresponding spin operator (S_x, S_y or S_z) on that axis, i.e. $\frac{\hbar}{2}$ or $-\frac{\hbar}{2}$. The quantum state of a particle (with respect to spin), can be represented by a two-component spinor:

$$\psi = \begin{pmatrix} a + bi \\ c + di \end{pmatrix}.$$

When the spin of this particle is measured with respect to a given axis (in this example, the x axis), the probability that its spin will be measured as $\frac{\hbar}{2}$ is just $\left|\langle \psi_{x+} | \psi \rangle\right|^2$. Correspondingly, the probability that its spin will be measured as $-\frac{\hbar}{2}$ is just $\left|\langle \psi_{x-} | \psi \rangle\right|^2$. Following the measurement, the spin state of the particle collapses into the corresponding eigenstate. As a result, if the particle's spin along a given axis has been measured to have a given eigenvalue, all measurements will yield the same eigenvalue (since $\left|\langle \psi_{x+} | \psi_{x+} \rangle\right|^2 = 1$, etc.), provided that no measurements of the spin are made along other axes.

Measurement of spin along an arbitrary axis

The operator to measure spin along an arbitrary axis direction is easily obtained from the Pauli spin matrices. Let $u = (u_x, u_y, u_z)$ be an arbitrary unit vector. Then the operator for spin in this direction is simply

$$S_u = \frac{\hbar}{2}(u_x\sigma_x + u_y\sigma_y + u_z\sigma_z).$$

The operator S_u has eigenvalues of $\pm\frac{\hbar}{2}$, just like the usual spin matrices. This method of finding the operator for spin in an arbitrary direction generalizes to higher spin states, one takes the dot product of the direction with a vector of the three operators for the three *x*-, *y*-, *z*-axis directions.

A normalized spinor for spin-$\frac{1}{2}$ in the (u_x, u_y, u_z) direction (which works for all spin states except spin down, where it will give $\frac{0}{0}$) is

$$\frac{1}{\sqrt{2+2u_z}}\begin{pmatrix} 1+u_z \\ u_x+iu_y \end{pmatrix}.$$

The above spinor is obtained in the usual way by diagonalizing the σ_u matrix and finding the eigenstates corresponding to the eigenvalues. In quantum mechanics, vectors are termed "normalized" when multiplied by a normalizing factor, which results in the vector having a length of unity.

Compatibility of spin measurements

Since the Pauli matrices do not commute, measurements of spin along the different axes are incompatible. This means that if, for example, we know the spin along the *x* axis, and we then measure the spin along the *y* axis, we have invalidated our previous knowledge of the *x* axis spin. This can be seen from the property of the eigenvectors (i.e. eigenstates) of the Pauli matrices that

$$\left|\langle\psi_{x\pm}|\psi_{y\pm}\rangle\right|^2 = \left|\langle\psi_{x\pm}|\psi_{z\pm}\rangle\right|^2 = \left|\langle\psi_{y\pm}|\psi_{z\pm}\rangle\right|^2 = \tfrac{1}{2}.$$

So when physicists measure the spin of a particle along the *x* axis as, for example, $\frac{\hbar}{2}$, the particle's spin state collapses into the eigenstate $|\psi_{x+}\rangle$. When we then subsequently measure the particle's spin along the *y* axis, the spin state will now collapse into either $|\psi_{y+}\rangle$ or $|\psi_{y-}\rangle$, each with probability $\frac{1}{2}$. Let us say, in our example, that we measure $-\frac{\hbar}{2}$. When we now return to measure the particle's spin along the *x* axis again, the probabilities that we will measure $\frac{\hbar}{2}$ or $-\frac{\hbar}{2}$ are each $\frac{1}{2}$ (i.e. they are $\left|\langle\psi_{x+}|\psi_{y-}\rangle\right|^2$ and $\left|\langle\psi_{x-}|\psi_{y-}\rangle\right|^2$ respectively). This implies that the original measurement of the spin along the *x* axis is no longer valid, since the spin along the *x* axis will now be measured to have either eigenvalue with equal probability.

Higher spins

The spin-$\frac{1}{2}$ operator $\mathbf{S} = \frac{\hbar}{2}\boldsymbol{\sigma}$ forms the fundamental representation of SU(2). By taking Kronecker products of this representation with itself repeatedly, one may construct all higher irreducible representations. That is, the resulting spin operators for higher-spin systems in three spatial dimensions can be calculated for arbitrarily large *s* using this spin operator and ladder operators. For example, taking the Kronecker product of two spin-$\frac{1}{2}$ yields a four-dimensional representation, which is separable into a 3-dimensional spin-1 (triplet states) and a 1-dimensional spin-0 representation (singlet state).

The resulting irreducible representations yield the following spin matrices and eigenvalues in the z-basis:

1. For spin 1 they are

$$S_x = \frac{\hbar}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad |1,+1\rangle_x = \frac{1}{2}\begin{pmatrix} 1 \\ \sqrt{2} \\ 1 \end{pmatrix}, \qquad |1,0\rangle_x = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \qquad |1,-1\rangle_x = \frac{1}{2}\begin{pmatrix} 1 \\ -\sqrt{2} \\ 1 \end{pmatrix}$$

$$S_y = \frac{\hbar}{\sqrt{2}}\begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix}, \qquad |1,+1\rangle_y = \frac{1}{2}\begin{pmatrix} -1 \\ -i\sqrt{2} \\ 1 \end{pmatrix}, \qquad |1,0\rangle_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad |1,-1\rangle_y = \frac{1}{2}\begin{pmatrix} -1 \\ i\sqrt{2} \\ 1 \end{pmatrix}$$

$$S_z = \hbar\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad |1,+1\rangle_z = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \qquad |1,0\rangle_z = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \qquad |1,-1\rangle_z = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

2. For spin $\frac{3}{2}$ they are

$$S_x = \tfrac{\hbar}{2}\begin{pmatrix} 0 & \sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & 2 & 0 \\ 0 & 2 & 0 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{pmatrix}, \qquad \left|\tfrac{3}{2},\tfrac{+3}{2}\right\rangle_x = \tfrac{1}{2\sqrt{2}}\begin{pmatrix} 1 \\ \sqrt{3} \\ \sqrt{3} \\ 1 \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{+1}{2}\right\rangle_x = \tfrac{1}{2\sqrt{2}}\begin{pmatrix} -\sqrt{3} \\ -1 \\ 1 \\ \sqrt{3} \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{-1}{2}\right\rangle_x = \tfrac{1}{2\sqrt{2}}\begin{pmatrix} \sqrt{3} \\ -1 \\ -1 \\ \sqrt{3} \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{-3}{2}\right\rangle_x =$$

$$S_y = \tfrac{\hbar}{2}\begin{pmatrix} 0 & -i\sqrt{3} & 0 & 0 \\ i\sqrt{3} & 0 & -2i & 0 \\ 0 & 2i & 0 & -i\sqrt{3} \\ 0 & 0 & i\sqrt{3} & 0 \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{+3}{2}\right\rangle_y = \tfrac{1}{2\sqrt{2}}\begin{pmatrix} i \\ -\sqrt{3} \\ -i\sqrt{3} \\ 1 \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{+1}{2}\right\rangle_y = \tfrac{1}{2\sqrt{2}}\begin{pmatrix} -i\sqrt{3} \\ 1 \\ -i \\ \sqrt{3} \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{-1}{2}\right\rangle_y = \tfrac{1}{2\sqrt{2}}\begin{pmatrix} i\sqrt{3} \\ 1 \\ i \\ \sqrt{3} \end{pmatrix}, \quad \left|\tfrac{3}{2},\tfrac{-3}{2}\right\rangle_y =$$

$$S_z = \tfrac{\hbar}{2}\begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix}, \qquad \left|\tfrac{3}{2},\tfrac{+3}{2}\right\rangle_z = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad \left|\tfrac{3}{2},\tfrac{+1}{2}\right\rangle_z = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \qquad \left|\tfrac{3}{2},\tfrac{-1}{2}\right\rangle_z = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \qquad \left|\tfrac{3}{2},\tfrac{-3}{2}\right\rangle_z =$$

3. For spin $\frac{5}{2}$ they are

$$S_x = \frac{\hbar}{2}\begin{pmatrix} 0 & \sqrt{5} & 0 & 0 & 0 & 0 \\ \sqrt{5} & 0 & 2\sqrt{2} & 0 & 0 & 0 \\ 0 & 2\sqrt{2} & 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 & 2\sqrt{2} & 0 \\ 0 & 0 & 0 & 2\sqrt{2} & 0 & \sqrt{5} \\ 0 & 0 & 0 & 0 & \sqrt{5} & 0 \end{pmatrix},$$

$$S_y = \frac{\hbar}{2}\begin{pmatrix} 0 & -i\sqrt{5} & 0 & 0 & 0 & 0 \\ i\sqrt{5} & 0 & -2i\sqrt{2} & 0 & 0 & 0 \\ 0 & 2i\sqrt{2} & 0 & -3i & 0 & 0 \\ 0 & 0 & 3i & 0 & -2i\sqrt{2} & 0 \\ 0 & 0 & 0 & 2i\sqrt{2} & 0 & -i\sqrt{5} \\ 0 & 0 & 0 & 0 & i\sqrt{5} & 0 \end{pmatrix},$$

$$S_z = \frac{\hbar}{2}\begin{pmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 & -5 \end{pmatrix}.$$

4. The generalization of these matrices for arbitrary spin s is

$$(S_x)_{ab} = \frac{\hbar}{2}\left(\delta_{a,b+1} + \delta_{a+1,b}\right)\sqrt{(s+1)(a+b-1) - ab},$$
$$(S_y)_{ab} = \frac{i\hbar}{2}\left(\delta_{a,b+1} - \delta_{a+1,b}\right)\sqrt{(s+1)(a+b-1) - ab},$$
$$(S_z)_{ab} = \hbar(s+1-a)\delta_{a,b} = \hbar(s+1-b)\delta_{a,b},$$

where indices a, b are integer numbers such that

$$1 \le a \le 2s+1, \quad 1 \le b \le 2s+1.$$

Also useful in the quantum mechanics of multiparticle systems, the general Pauli group G_n is defined to consist of all n-fold tensor products of Pauli matrices.

The analog formula of Euler's formula in terms of the Pauli matrices

$$\hat{R}(\theta, \hat{\mathbf{n}}) = e^{i\frac{\theta}{2}\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}} = I\cos\frac{\theta}{2} + i\left(\hat{\mathbf{n}}\cdot\boldsymbol{\sigma}\right)\sin\frac{\theta}{2}$$

for higher spins is tractable, but less simple.[26]

Parity

In tables of the spin quantum number s for nuclei or particles, the spin is often followed by a "+" or "−". This refers to the parity with "+" for even parity (wave function unchanged by spatial inversion) and "−" for odd parity (wave function negated by spatial inversion). For example, see the isotopes of bismuth, in which the list of isotopes includes the column nuclear spin and parity. For Bi-209, the longest-lived isotope, the entry 9/2– means that the nuclear spin is 9/2 and the parity is odd.

Measuring spin

The nuclear spin of atoms can be determined by sophisticated improvements to the original Stern-Gerlach experiment.[27] A single-energy (monochromatic) molecular beam of atoms in an inhomogeneous magnetic field will split into beams representing each possible spin quantum state. For an atom with electronic spin S and nuclear spin I, there are $(2S + 1)(2I + 1)$ spin states. For example, neutral Na atoms, which have $S = 1/2$, were passed through a series of inhomogeneous magnetic fields that selected one of the two electronic spin states and separated the nuclear spin states, from which four beams were observed. Thus, the nuclear spin for ^{23}Na atoms was found to be $I = 3/2$.[28][29]

The spin of pions, a type of elementary particle, was determined by the principle of detailed balance applied to those collisions of protons that produced charged pions and deuterium.

$$p + p \to \pi_- + d$$

The known spin values for protons and deuterium allows analysis of the collision cross-section to show that π_- has spin $s_\pi = 0$. A different approach is needed for neutral pions. In that case the decay reaction into two gamma ray photons with spin one:

$$\pi_0 \to 2\gamma$$

This results supplemented with additional analysis leads to the conclusion that the neutral pion also has spin zero.[30]:66

Applications

Spin has important theoretical implications and practical applications. Well-established *direct* applications of spin include:

- Nuclear magnetic resonance (NMR) spectroscopy in chemistry;
- Electron spin resonance (ESR or EPR) spectroscopy in chemistry and physics;
- Magnetic resonance imaging (MRI) in medicine, a type of applied NMR, which relies on proton spin density;
- Giant magnetoresistive (GMR) drive-head technology in modern hard disks.

Electron spin plays an important role in magnetism, with applications for instance in computer memories. The manipulation of *nuclear spin* by radio-frequency waves (nuclear magnetic resonance) is important in chemical spectroscopy and medical imaging.

Spin–orbit coupling leads to the fine structure of atomic spectra, which is used in atomic clocks and in the modern definition of the second. Precise measurements of the g-factor of the electron have played an important role in the development and verification of quantum electrodynamics. *Photon spin* is associated with the polarization of light (photon polarization).

An emerging application of spin is as a binary information carrier in spin transistors. The original concept, proposed in 1990, is known as Datta–Das spin transistor.[31] Electronics based on spin transistors are referred to as spintronics. The manipulation of spin in dilute magnetic semiconductor materials, such as metal-doped ZnO or TiO_2 imparts a further degree of freedom and has the potential to facilitate the fabrication of more efficient electronics.[32]

There are many *indirect* applications and manifestations of spin and the associated Pauli exclusion principle, starting with the periodic table of chemistry.

History

Spin was first discovered in the context of the emission spectrum of alkali metals. Starting around 1910, many experiments on different atoms produced a collection of relationships involving quantum numbers for atomic energy levels partially summarized in Bohr's model for the atom[33]:106 Transitions between levels obeyed selection rules and the rules were known to be correlated with even or odd atomic number. Additional information was known from changes to atomic spectra observed in strong magnetic fields, known as the Zeeman effect. In 1924, Wolfgang Pauli used this large collection of empirical observations to propose a new degree of freedom,[7] introducing what he called a "two-valuedness not describable classically"[34] associated with the electron in the outermost shell.


Wolfgang Pauli lecturing

The physical interpretation of Pauli's "degree of freedom" was initially unknown. Ralph Kronig, one of Alfred Landé's assistants, suggested in early 1925 that it was produced by the self-rotation of the electron. When Pauli heard about the idea, he criticized it severely, noting that the electron's hypothetical surface would have to be moving faster than the speed of light in order for it to rotate quickly enough to produce the necessary angular momentum. This would violate the theory of relativity. Largely due to Pauli's criticism, Kronig decided not to publish his idea.[35]

In the autumn of 1925, the same thought came to Dutch physicists George Uhlenbeck and Samuel Goudsmit at Leiden University. Under the advice of Paul Ehrenfest, they published their results.[36] The young physicists immediately regretted the publication: Hendrik Lorentz and Werner Heisenberg both pointed out problems with the concept of a spinning electron.[37]

Pauli was especially unconvinced and continued to pursue his two-valued degree of freedom. This allowed him to formulate the Pauli exclusion principle, stating that no two electrons can have the same quantum state in the same quantum system.

Fortunately by February 1926 Llewellyn Thomas managed to resolve a factor-of-two discrepancy between experimental results for the fine structure in the hydrogen spectrum and calculations based on Uhlenbeck and Goudsmit's (and Kronig's unpublished) model.[2]:385 This discrepancy was due to a relativistic effect, the difference between the electron's rotating rest frame and the nuclear rest frame; the effect is now known as Thomas precession.[7] Thomas' result convinced Pauli that electron spin was the correct interpretation of his two-valued degree of freedom, while he continued to insist that the classical rotating charge model is invalid.[34][6]

In 1927 Pauli formalized the theory of spin using the theory of quantum mechanics invented by Erwin Schrödinger and Werner Heisenberg. He pioneered the use of Pauli matrices as a representation of the spin operators and introduced a two-component spinor wave-function.

Pauli's theory of spin was non-relativistic. In 1928, Paul Dirac published his relativistic electron equation, using a four-component spinor (known as a "Dirac spinor") for the electron wave-function. Relativistic spin explained gyromagnetic anomaly. In 1940, Pauli proved the *spin–statistics theorem*, which states that fermions have half-integer spin, and bosons have integer spin.[7]

In retrospect, the first direct experimental evidence of the electron spin was the Stern–Gerlach experiment of 1922. However, the correct explanation of this experiment was only given in 1927.[38] The original interpretation assumed the two spots observed in the experiment were due to quantized orbital angular momentum. However, in 1927 Ronald Fraser showed that Sodium atoms are isotropic with no orbital angular momentum and suggested that the observed magnetic properties were due to electron spin.[39] In same year, Phipps and Taylor applied the Stern-Gerlach technique to hydrogen atoms; the ground state of hydrogen has zero angular momentum but the measurements again showed two peaks.[40] Once the quantum theory became established, it became clear that the original interpretation could not have been correct: the possible values of orbital angular momentum along one axis is always an odd number, unlike the observations. Hydrogen atoms have a single electron with two spin states giving the two spots observed; silver atoms have closed shells which do not contribute to the magnetic moment and only the unmatched outer electron's spin responds to the field.

See also

- Chirality (physics)
- Dynamic nuclear polarization
- Helicity (particle physics)
- Holstein–Primakoff transformation
- Kramers' theorem
- Pauli equation
- Pauli–Lubanski pseudovector
- Rarita–Schwinger equation
- Representation theory of SU(2)
- Spin angular momentum of light
- Spin engineering
- Spin-flip

- Spin isomers of hydrogen
- Spin–orbit interaction
- Spin tensor
- Spintronics
- Spin wave
- Yrast

References

1. Merzbacher, Eugen (1998). *Quantum Mechanics* (https://archive.org/details/quantummechanics00merz_136) (3rd ed.). John Wiley & Sons. pp. 372 (https://archive.org/details/quantummechanics00merz_136/page/n385)–373. ISBN 978-0-471-88702-7.
2. Griffiths, David (2005). *Introduction to Quantum Mechanics* (https://archive.org/details/introductiontoqu00grif_190) (2nd ed.).
3. Eisberg, Robert; Resnick, Robert (1985). *Quantum Physics of Atoms, Molecules, Solids, Nuclei, and Particles* (https://archive.org/details/quantumphysicsat00eisb) (2nd ed.). Wiley. pp. 272 (https://archive.org/details/quantumphysicsat00eisb/page/n288)–273. ISBN 978-0-471-87373-0.
4. Sebens, Charles T. (November 2019). "How electrons spin" (https://linkinghub.elsevier.com/retrieve/pii/S135521981830087X). *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*. **68**: 40–50. arXiv:1806.01121 (https://arxiv.org/abs/1806.01121). doi:10.1016/j.shpsb.2019.04.007 (https://doi.org/10.1016%2Fj.shpsb.2019.04.007). S2CID 51693779 (https://api.semanticscholar.org/CorpusID:51693779).
5. "Fermilab Today" (https://www.fnal.gov/pub/today/archive/archive_2013/today13-02-15_NutshellReadMore.html). *www.fnal.gov*. Retrieved 2023-06-16.
6. Giulini, Domenico (2008-09-01). "Electron spin or "classically non-describable two-valuedness" " (https://www.sciencedirect.com/science/article/pii/S1355219808000269). *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*. **39** (3): 557–578. arXiv:0710.3128 (https://arxiv.org/abs/0710.3128). doi:10.1016/j.shpsb.2008.03.005 (https://doi.org/10.1016%2Fj.shpsb.2008.03.005). ISSN 1355-2198 (https://search.worldcat.org/issn/1355-2198).
7. Fröhlich, Jürg (2009). "Spin, or actually: Spin and Quantum Statistics". In Duplantier, Bertrand; Raimond, Jean-Michel; Rivasseau, Vincent (eds.). *The Spin. Progress in Mathematical Physics, vol 55* (http://link.springer.com/10.1007/978-3-7643-8799-0_1). Basel: Birkhäuser Basel. pp. 1–60. doi:10.1007/978-3-7643-8799-0_1 (https://doi.org/10.1007%2F978-3-7643-8799-0_1). ISBN 978-3-7643-8798-3.
8. Leader, Elliot; Lorcé, Cédric (2014-08-20). "The angular momentum controversy: What's it all about and does it matter?" (https://www.sciencedirect.com/science/article/pii/S0370157314001185). *Physics Reports*. The angular momentum controversy: What's it all about and does it matter?. **541** (3): 163–248. arXiv:1309.4235 (https://arxiv.org/abs/1309.4235). doi:10.1016/j.physrep.2014.02.010 (https://doi.org/10.1016%2Fj.physrep.2014.02.010). ISSN 0370-1573 (https://search.worldcat.org/issn/0370-1573).
9. Peskin, M. E., & Schroeder, D. V. (1995). *Quantum field theory*, Ch. 3. The Advanced Book Program.
10. Ohanian, Hans C. (1986-06-01). "What is spin?" (https://physics.mcmaster.ca/phys3mm3/notes/whatisspin.pdf) (PDF). *American Journal of Physics*. **54** (6): 500–505. Bibcode:1986AmJPh..54..500O (https://ui.adsabs.harvard.edu/abs/1986AmJPh..54..500O). doi:10.1119/1.14580 (https://doi.org/10.1119%2F1.14580). ISSN 0002-9505 (https://search.worldcat.org/issn/0002-9505).
11. Bliokh, Konstantin Y.; Punzmann, Horst; Xia, Hua; Nori, Franco; Shats, Michael (2022-01-21). "Field theory spin and momentum in water waves" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8782445). *Science Advances*. **8** (3): eabm1295. Bibcode:2022SciA....8.1295B (https://ui.adsabs.harvard.edu/abs/2022SciA....8.1295B). doi:10.1126/sciadv.abm1295 (https://doi.org/10.1126%2Fsciadv.abm1295). ISSN 2375-2548 (https://search.worldcat.org/issn/2375-2548). PMC 8782445 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8782445). PMID 35061526 (https://pubmed.ncbi.nlm.nih.gov/35061526).
12. Whittaker, Sir Edmund (1989-01-01). *A History of the Theories of Aether and Electricity*. Vol. 2. Courier Dover Publications. p. 87. ISBN 0-486-26126-3.
13. Information about Higgs Boson (http://home.cern/topics/higgs-boson) in CERN's official website.
14. Pauli, Wolfgang (1940). "The Connection Between Spin and Statistics" (http://hermes.ffn.ub.es/luisnavarro/nuevo_maletin/Pauli_spin_statistics_1940.pdf) (PDF). *Phys. Rev*. **58** (8): 716–722. Bibcode:1940PhRv...58..716P (https://ui.adsabs.harvard.edu/abs/1940PhRv...58..716P). doi:10.1103/PhysRev.58.716 (https://doi.org/10.1103%2FPhysRev.58.716).
15. Physics of Atoms and Molecules, B. H. Bransden, C. J. Joachain, Longman, 1983, ISBN 0-582-44401-2.
16. "2022 CODATA Value: electron g factor" (https://physics.nist.gov/cgi-bin/cuu/Value?gem). *The NIST Reference on Constants, Units, and Uncertainty*. NIST. May 2024. Retrieved 2024-05-18.
17. Feynman, R. P. (1985). "Electrons and their interactions". *QED: The Strange Theory of Light and Matter*. Princeton, New Jersey: Princeton University Press. p. 115. ISBN 978-0-691-08388-9. "After some years, it was discovered that this value [$-\frac{1}{2}\ g$] was not exactly 1, but slightly more – something like 1.00116. This correction was worked out for the first time in 1948 by Schwinger as $j \times j$ divided by 2π [*sic*] [where j is the square root of the fine-structure constant], and was due to an alternative way the electron can go from place to place: Instead of going directly from one point to another, the electron goes along for a while and suddenly emits a photon; then (horrors!) it absorbs its own photon."
18. Marciano, W. J.; Sanda, A. I. (1977). "Exotic decays of the muon and heavy leptons in gauge theories". *Physics Letters*. **B67** (3): 303–305. Bibcode:1977PhLB...67..303M (https://ui.adsabs.harvard.edu/abs/1977PhLB...67..303M). doi:10.1016/0370-2693(77)90377-X (https://doi.org/10.1016%2F0370-2693%2877%2990377-X).
19. Lee, B. W.; Shrock, R. E. (1977). "Natural suppression of symmetry violation in gauge theories: Muon- and electron-lepton-number nonconservation". *Physical Review*. **D16** (5): 1444–1473. Bibcode:1977PhRvD..16.1444L (https://ui.adsabs.harvard.edu/abs/1977PhRvD..16.1444L). doi:10.1103/PhysRevD.16.1444 (https://doi.org/10.1103%2FPhysRevD.16.1444). S2CID 1430757 (https://api.semanticscholar.org/CorpusID:1430757).
20. K. Fujikawa; R. E. Shrock (1980). "Magnetic Moment of a Massive Neutrino and Neutrino-Spin Rotation". *Physical Review Letters*. **45** (12): 963–966. Bibcode:1980PhRvL..45..963F (https://ui.adsabs.harvard.edu/abs/1980PhRvL..45..963F). doi:10.1103/PhysRevLett.45.963 (https://doi.org/10.1103%2FPhysRevLett.45.963).
21. Bell, N. F.; Cirigliano, V.; Ramsey-Musolf, M.; Vogel, P.; Wise, Mark; et al. (2005). "How Magnetic is the Dirac neutrino?". *Physical Review Letters*. **95** (15): 151802. arXiv:hep-ph/0504134 (https://arxiv.org/abs/hep-ph/0504134). Bibcode:2005PhRvL..95o1802B (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95o1802B). doi:10.1103/PhysRevLett.95.151802 (https://doi.org/10.1103%2FPhysRevLett.95.151802). PMID 16241715 (https://pubmed.ncbi.nlm.nih.gov/16241715). S2CID 7832411 (https://api.semanticscholar.org/CorpusID:7832411).
22. Quanta: A handbook of concepts, P. W. Atkins, Oxford University Press, 1974, ISBN 0-19-855493-1.
23. Messiah, Albert (2014). "Angular Momentum in Quantum Mechanics". *Quantum Mechanics*. Mineola, NY: Dover Publications. p. 540. ISBN 978-1-306-51279-4. OCLC 874097814 (https://search.worldcat.org/oclc/874097814).
24. B. C. Hall (2013). *Quantum Theory for Mathematicians*. Springer. pp. 354–358.
25. Sakurai, Jun John; Napolitano, Jim (2017). *Modern quantum mechanics* (https://www.academia.edu/download/64391583/modern%20quantum%20mechanics.pdf) (PDF) (2nd ed.). Cambridge: Cambridge university press. ISBN 978-1-108-42241-3.
26. Curtright, T. L.; Fairlie, D. B.; Zachos, C. K. (2014). "A compact formula for rotations as spin matrix polynomials". *SIGMA*. **10**: 084. arXiv:1402.3541 (https://arxiv.org/abs/1402.3541). Bibcode:2014SIGMA..10..084C (https://ui.adsabs.harvard.edu/abs/2014SIGMA..10..084C). doi:10.3842/SIGMA.2014.084 (https://doi.org/10.3842%2FSIGMA.2014.084). S2CID 18776942 (https://api.semanticscholar.org/CorpusID:18776942).

27. Hamilton, Donald R. (1941-12-01). "Molecular Beams and Nuclear Moments" (https://pubs.aip.org/ajp/article/9/6/319/1037623/Molecular-Beams-and-Nuclear-Moments). *American Journal of Physics*. **9** (6): 319–337. doi:10.1119/1.1991712 (https://doi.org/10.1119%2F1.1991712). ISSN 0002-9505 (https://search.worldcat.org/issn/0002-9505).
28. Rabi, I. I.; Cohen, V. W. (1933-04-01). "The Nuclear Spin of Sodium" (https://link.aps.org/doi/10.1103/PhysRev.43.582). *Physical Review*. **43** (7): 582–583. doi:10.1103/PhysRev.43.582 (https://doi.org/10.1103%2FPhysRev.43.582). ISSN 0031-899X (https://search.worldcat.org/issn/0031-899X).
29. Estermann, I. (1946-07-01). "Molecular Beam Technique" (https://link.aps.org/doi/10.1103/RevModPhys.18.300). *Reviews of Modern Physics*. **18** (3): 300–323. doi:10.1103/RevModPhys.18.300 (https://doi.org/10.1103%2FRevModPhys.18.300). ISSN 0034-6861 (https://search.worldcat.org/issn/0034-6861).
30. Perkins, Donald H. (2008). *Introduction to high energy physics* (4. Aufl., 8. print ed.). Cambridge: Cambridge Univ. Press. ISBN 978-0-521-62196-0.
31. Datta, S.; Das, B. (1990). "Electronic analog of the electrooptic modulator". *Applied Physics Letters*. **56** (7): 665–667. Bibcode:1990ApPhL..56..665D (https://ui.adsabs.harvard.edu/abs/1990ApPhL..56..665D). doi:10.1063/1.102730 (https://doi.org/10.1063%2F1.102730).
32. Assadi, M. H. N.; Hanaor, D. A. H. (2013). "Theoretical study on copper's energetics and magnetism in TiO_2 polymorphs". *Journal of Applied Physics*. **113** (23): 233913–233913–5. arXiv:1304.1854 (https://arxiv.org/abs/1304.1854). Bibcode:2013JAP...113w3913A (https://ui.adsabs.harvard.edu/abs/2013JAP...113w3913A). doi:10.1063/1.4811539 (https://doi.org/10.1063%2F1.4811539). S2CID 94599250 (https://api.semanticscholar.org/CorpusID:94599250).
33. Whittaker, Edmund T. (1989). *A history of the theories of aether & electricity. 2: The modern theories, 1900 - 1926* (Repr ed.). New York: Dover Publ. ISBN 978-0-486-26126-3.
34. Wolfgang Pauli (December 13, 1946). "Exclusion Principle and Quantum Mechanics" (https://www.nobelprize.org/prizes/physics/1945/pauli/lecture/). *Nobel Lecture*. Nobel Prize.
35. Pais, Abraham (1991). *Niels Bohr's Times* (https://archive.org/details/nielsbohrstimesi00pais_0). Oxford: Clarendon Press. pp. 244 (https://archive.org/details/nielsbohrstimesi00pais_0/page/244). ISBN 978-0-19-852049-8.
36. Uhlenbeck, G., G.; Goudsmit, S. (November 1925). "Ersetzung der Hypothese vom unmechanischen Zwang durch eine Forderung bezüglich des inneren Verhaltens jedes einzelnen Elektrons". *Die Naturwissenschaften* (in German). **13** (47): 953–954. doi:10.1007/bf01558878 (https://doi.org/10.1007%2Fbf01558878). ISSN 0028-1042 (https://search.worldcat.org/issn/0028-1042). S2CID 32211960 (https://api.semanticscholar.org/CorpusID:32211960).
37. Pais, Abraham (1989-12-01). "George Uhlenbeck and the Discovery of Electron Spin" (https://pubs.aip.org/physicstoday/article/42/12/34/405387/George-Uhlenbeck-and-the-Discovery-of-Electron). *Physics Today*. **42** (12): 34–40. doi:10.1063/1.881186 (https://doi.org/10.1063%2F1.881186). ISSN 0031-9228 (https://search.worldcat.org/issn/0031-9228).
38. B. Friedrich; D. Herschbach (2003). "Stern and Gerlach: How a Bad Cigar Helped Reorient Atomic Physics" (https://doi.org/10.1063%2F1.1650229). *Physics Today*. **56** (12): 53. Bibcode:2003PhT....56l..53F (https://ui.adsabs.harvard.edu/abs/2003PhT....56l..53F). doi:10.1063/1.1650229 (https://doi.org/10.1063%2F1.1650229). S2CID 17572089 (https://api.semanticscholar.org/CorpusID:17572089).
39. "The effective cross section of the oriented hydrogen atom" (https://royalsocietypublishing.org/doi/10.1098/rspa.1927.0036). *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*. **114** (767): 212–221. March 1927. doi:10.1098/rspa.1927.0036 (https://doi.org/10.1098%2Frspa.1927.0036). ISSN 0950-1207 (https://search.worldcat.org/issn/0950-1207).
40. Resnick, R.; Eisberg, R. (1985). *Quantum Physics of Atoms, Molecules, Solids, Nuclei and Particles* (https://archive.org/details/quantumphysicsof00eisb/page/274) (2nd ed.). John Wiley & Sons. p. 274 (https://archive.org/details/quantumphysicsof00eisb/page/274). ISBN 978-0-471-87373-0.

Further reading

- Cohen-Tannoudji, Claude; Diu, Bernard; Laloë, Franck (2006). *Quantum Mechanics* (2 volume set ed.). John Wiley & Sons. ISBN 978-0-471-56952-7.
- Condon, E. U.; Shortley, G. H. (1935). "Especially Chapter 3". *The Theory of Atomic Spectra*. Cambridge University Press. ISBN 978-0-521-09209-8.
- Hipple, J. A.; Sommer, H.; Thomas, H.A. (1949). "A precise method of determining the faraday by magnetic resonance" (https://www.academia.edu/6483539). *Physical Review*. **76** (12): 1877–1878. Bibcode:1949PhRv...76.1877H (https://ui.adsabs.harvard.edu/abs/1949PhRv...76.1877H). doi:10.1103/PhysRev.76.1877.2 (https://doi.org/10.1103%2FPhysRev.76.1877.2).
- Edmonds, A. R. (1957). *Angular Momentum in Quantum Mechanics* (https://archive.org/details/angularmomentumi0000edmo). Princeton University Press. ISBN 978-0-691-07912-7.
- Jackson, John David (1998). *Classical Electrodynamics* (3rd ed.). John Wiley & Sons. ISBN 978-0-471-30932-1.
- Serway, Raymond A.; Jewett, John W. (2004). *Physics for Scientists and Engineers* (https://archive.org/details/physicssciengv2p00serw) (6th ed.). Brooks/Cole. ISBN 978-0-534-40842-8.
- Thompson, William J. (1994). *Angular Momentum: An Illustrated Guide to Rotational Symmetries for Physical Systems*. Wiley. ISBN 978-0-471-55264-2.
- Tipler, Paul (2004). *Physics for Scientists and Engineers: Mechanics, Oscillations and Waves, Thermodynamics* (5th ed.). W. H. Freeman. ISBN 978-0-7167-0809-4.
- Sin-Itiro Tomonaga, The Story of Spin, 1997

External links

- Quotations related to Spin (physics) at Wikiquote
- Goudsmit on the discovery of electron spin. (http://www.lorentz.leidenuniv.nl/history/spin/goudsmit.html)
- *Nature*: "Milestones in 'spin' since 1896. (https://www.nature.com/collections/idgejiafca)"
- ECE 495N Lecture 36: Spin (http://nanohub.org/resources/6025) Online lecture by S. Datta

Retrieved from "https://en.wikipedia.org/w/index.php?title=Spin_(physics)&oldid=1237526517"

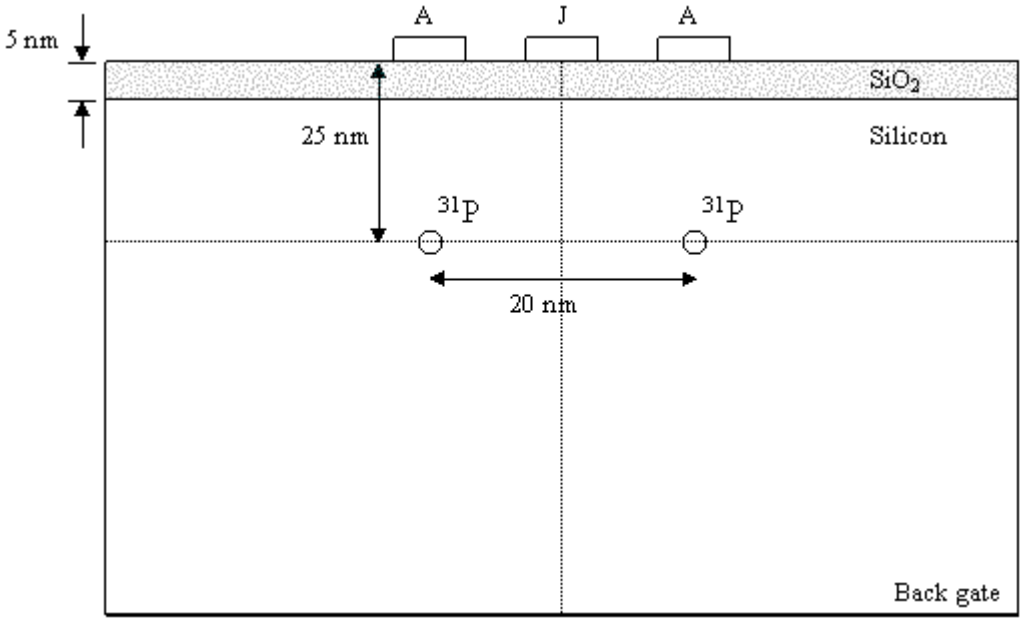
WIKIPEDIA
The Free Encyclopedia

Kane quantum computer

The Kane quantum computer is a proposal for a scalable quantum computer proposed by Bruce Kane in 1998,[1] who was then at the University of New South Wales. Often thought of as a hybrid between quantum dot and nuclear magnetic resonance (NMR) quantum computers, the Kane computer is based on an array of individual phosphorus donor atoms embedded in a pure silicon lattice. Both the nuclear spins of the donors and the spins of the donor electrons participate in the computation.

Unlike many quantum computation schemes, the Kane quantum computer is in principle scalable to an arbitrary number of qubits. This is possible because qubits may be individually addressed by electrical means.

Description



The original proposal calls for phosphorus donors to be placed in an array with a spacing of 20 nm, approximately 20 nm below the surface. An insulating oxide layer is grown on top of the silicon. Metal **A gates** are deposited on the oxide above each donor, and **J gates** between adjacent donors.

The phosphorus donors are isotopically pure ^{31}P, which have a nuclear spin of 1/2. The silicon substrate is isotopically pure ^{28}Si which has nuclear spin 0. Using the nuclear spin of the P donors as a method to encode qubits has two major advantages. Firstly, the state has an extremely long decoherence time, perhaps on the order of 10^{18} seconds at millikelvin temperatures. Secondly, the qubits may be manipulated by applying an oscillating magnetic field, as in typical NMR proposals. By altering the voltage on the A gates, it should be possible to alter the Larmor frequency of individual donors. This allows them to be addressed individually, by bringing specific donors into resonance with the applied oscillating magnetic field.

Nuclear spins alone will not interact significantly with other nuclear spins 20 nm away. Nuclear spin is useful to perform single-qubit operations, but to make a quantum computer, two-qubit operations are also required. This is the role of electron spin in this design. Under A-gate control, the spin is transferred from the nucleus to the donor electron. Then, a potential is applied to the J gate, drawing adjacent donor electrons into a common region, greatly enhancing the interaction between the neighbouring spins. By controlling the J gate voltage, two-qubit operations are possible.

Kane's proposal for readout was to apply an electric field to encourage spin-dependent tunneling of an electron to transform two neutral donors to a D^+–D^- state, that is, one where two electrons associate with the same donor. The charge excess is then detected using a single-electron transistor. This method has two major difficulties. Firstly, the D^- state has strong coupling with the environment and hence a short decoherence time. Secondly and perhaps more importantly, it's not clear that the D^- state has a sufficiently long lifetime to allow for readout—the electron tunnels into the conduction band.

Development

Since Kane's proposal, under the guidance of Robert Clark and now Michelle Simmons, pursuing realisation of the Kane quantum computer has become the primary quantum computing effort in Australia.[2] Theorists have put forward a number of proposals for improved readout. Experimentally, atomic-precision deposition of phosphorus atoms has been achieved using a scanning tunneling microscope (STM) technique in 2003.[3] Detection of the movement of single electrons between small, dense clusters of phosphorus donors has also been achieved. The group remains optimistic that a practical large-scale quantum computer can be built. Other groups believe that the idea needs to be modified.[4]

In 2020, Andrea Morello and others demonstrated that an antimony nucleus (with eight spin states) embedded in silicon could be controlled using an electric field, rather than a magnetic field.[5]

See also

- Spin qubit quantum computer
- Nuclear magnetic resonance quantum computer

References

1. Kane, B.E. (1998)"A silicon-based nuclear spin quantum computer (http://www.nature.com/nature/journal/v393/n6681/abs/393133a0.html)", *Nature*, **393**, p133
2. Centre for Quantum Computation & Communication Technology (http://www.cqc2t.org/)
3. Schofield, S. R. Atomically precise placement of single dopants in Si. arXiv:cond-mat/0307599 (https://arxiv.org/abs/cond-mat/0307599) 2003
4. O'Gorman, J. A silicon-based surface code quantum computer. arXiv:1406.5149 (https://arxiv.org/abs/1406.5149) 2014
5. Cho, Adrian (11 March 2020). "Chance discovery brings quantum computing using standard microchips a step closer" (https://www.science.org/content/article/chance-discovery-brings-quantum-computing-using-standard-microchips-step-closer). *Science* | *AAAS*. Retrieved 13 March 2020.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Kane_quantum_computer&oldid=1189771881"

WIKIPEDIA
The Free Encyclopedia

Spin qubit quantum computer

The **spin qubit quantum computer** is a quantum computer based on controlling the spin of charge carriers (electrons and electron holes) in semiconductor devices.[1] The first spin qubit quantum computer was first proposed by Daniel Loss and David P. DiVincenzo in 1997,[1][2] also known as the **Loss–DiVincenzo quantum computer**. The proposal was to use the intrinsic spin-1/2 degree of freedom of individual electrons confined in quantum dots as qubits. This should not be confused with other proposals that use the nuclear spin as qubit, like the Kane quantum computer or the nuclear magnetic resonance quantum computer. Intel has developed quantum computers based on silicon spin qubits, also called hot qubits.[3][4][5]

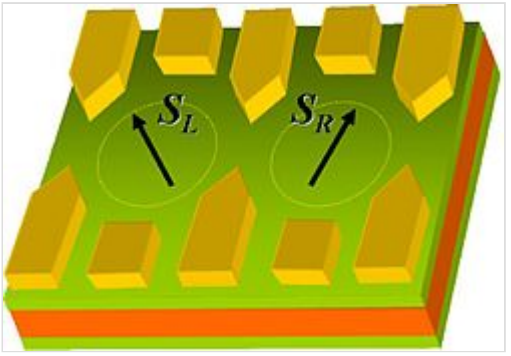
Spin qubits so far have been implemented by locally depleting two-dimensional electron gases in semiconductors such a gallium arsenide,[6][7] silicon[8] and germanium.[9] Spin qubits have also been implemented in graphene.[10]

Loss–DiVicenzo proposal

The Loss–DiVicenzo quantum computer proposal tried to fulfill DiVincenzo's criteria for a scalable quantum computer,[11] namely:

- identification of well-defined qubits;
- reliable state preparation;
- low decoherence;
- accurate quantum gate operations and
- strong quantum measurements.

A candidate for such a quantum computer is a lateral quantum dot system. Earlier work on applications of quantum dots for quantum computing was done by Barenco et al.[12]



A double quantum dot. Each electron spin S_L or S_R define one quantum two-level system, or a spin *qubit* in the Loss-DiVincenzo proposal. A narrow gate between the two dots can modulate the coupling, allowing swap operations.

Implementation of the two-qubit gate

The Loss–DiVincenzo quantum computer operates, basically, using inter-dot gate voltage for implementing swap operations and local magnetic fields (or any other local spin manipulation) for implementing the controlled NOT gate (CNOT gate).

The swap operation is achieved by applying a pulsed inter-dot gate voltage, so the exchange constant in the Heisenberg Hamiltonian becomes time-dependent:

$$H_s(t) = J(t)\mathbf{S_L} \cdot \mathbf{S_R}.$$

This description is only valid if:

- the level spacing in the quantum-dot ΔE is much greater than kT

- the pulse time scale τ_s is greater than $\hbar/\Delta E$, so there is no time for transitions to higher orbital levels to happen and
- the decoherence time Γ^{-1} is longer than τ_s.

k is the Boltzmann constant and T is the temperature in Kelvin.

From the pulsed Hamiltonian follows the time evolution operator

$$U_s(t) = \mathcal{T} \exp\left\{-i \int_0^t dt' H_s(t')\right\},$$

where $\mathcal{T}$ is the time-ordering symbol.

We can choose a specific duration of the pulse such that the integral in time over $J(t)$ gives $J_0 \tau_s = \pi \pmod{2\pi}$, and U_s becomes the swap operator $U_s(J_0\tau_s = \pi) \equiv U_{sw}$.

This pulse run for half the time (with $J_0\tau_s = \pi/2$) results in a square root of swap gate, $U_{sw}^{1/2}$.

The "XOR" gate may be achieved by combining $U_{sw}^{1/2}$ operations with individual spin rotation operations:

$$U_{XOR} = e^{i\frac{\pi}{2}S_L^z} e^{-i\frac{\pi}{2}S_R^z} U_{sw}^{1/2} e^{i\pi S_L^z} U_{sw}^{1/2}.$$

The U_{XOR} operator is a conditional phase shift (controlled-Z) for the state in the basis of $\mathbf{S_L} + \mathbf{S_R}$.[2]:4 It can be made into a CNOT gate by surrounding the desired target qubit with Hadamard gates.

See also

- Kane quantum computer
- Quantum dot cellular automaton

References

1. Vandersypen, Lieven M. K.; Eriksson, Mark A. (2019-08-01). "Quantum computing with semiconductor spins" (https://physicstoday.scitation.org/doi/abs/10.1063/PT.3.4270). *Physics Today*. **72** (8): 38. Bibcode:2019PhT....72h..38V (https://ui.adsabs.harvard.edu/abs/2019PhT....72h..38V). doi:10.1063/PT.3.4270 (https://doi.org/10.1063%2FPT.3.4270). ISSN 0031-9228 (https://search.worldcat.org/issn/0031-9228). S2CID 201305644 (https://api.semanticscholar.org/CorpusID:201305644).
2. Loss, Daniel; DiVincenzo, David P. (1998-01-01). "Quantum computation with quantum dots" (https://doi.org/10.1103%2Fphysreva.57.120). *Physical Review A*. **57** (1): 120–126. arXiv:cond-mat/9701055 (https://arxiv.org/abs/cond-mat/9701055). Bibcode:1998PhRvA..57..120L (https://ui.adsabs.harvard.edu/abs/1998PhRvA..57..120L). doi:10.1103/physreva.57.120 (https://doi.org/10.1103%2Fphysreva.57.120). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947).
3. "Intel releases 12-qubit silicon quantum chip to the quantum community" (https://physicsworld.com/a/intel-releases-12-qubit-silicon-quantum-chip-to-the-quantum-community/). 22 June 2023.

4. "Intel Enters the Quantum Computing Horse Race with 12-Qubit Chip" (https://www.cnet.com/tech/computing/intel-enters-the-quantum-computing-horse-race-with-12-qubit-chip/).
5. "What Intel is Planning for the Future of Quantum Computing: Hot Qubits, Cold Control Chips, and Rapid Testing - IEEE Spectrum" (https://spectrum.ieee.org/intels-quantum-computing-plans-hot-qubits-cold-control-chips-and-rapid-testing).
6. Petta, J. R. (2005). "Coherent Manipulation of Coupled Electron Spins in Semiconductor Quantum Dots". *Science*. **309** (5744): 2180–2184. Bibcode:2005Sci...309.2180P (https://ui.adsabs.harvard.edu/abs/2005Sci...309.2180P). doi:10.1126/science.1116955 (https://doi.org/10.1126%2Fscience.1116955). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 16141370 (https://pubmed.ncbi.nlm.nih.gov/16141370). S2CID 9107033 (https://api.semanticscholar.org/CorpusID:9107033).
7. Bluhm, Hendrik; Foletti, Sandra; Neder, Izhar; Rudner, Mark; Mahalu, Diana; Umansky, Vladimir; Yacoby, Amir (2010). "Dephasing time of GaAs electron-spin qubits coupled to a nuclear bath exceeding 200 μs" (https://doi.org/10.1038%2Fnphys1856). *Nature Physics*. **7** (2): 109–113. doi:10.1038/nphys1856 (https://doi.org/10.1038%2Fnphys1856). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473).
8. Wang, Siying; Querner, Claudia; Dadosh, Tali; Crouch, Catherine H.; Novikov, Dmitry S.; Drndic, Marija (2011). "Collective fluorescence enhancement in nanoparticle clusters" (https://doi.org/10.1038%2Fncomms1357). *Nature Communications*. **2** (1): 364. Bibcode:2011NatCo...2..364W (https://ui.adsabs.harvard.edu/abs/2011NatCo...2..364W). doi:10.1038/ncomms1357 (https://doi.org/10.1038%2Fncomms1357). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMID 21694712 (https://pubmed.ncbi.nlm.nih.gov/21694712).
9. Watzinger, Hannes; Kukučka, Josip; Vukušić, Lada; Gao, Fei; Wang, Ting; Schäffler, Friedrich; Zhang, Jian-Jun; Katsaros, Georgios (2018-09-25). "A germanium hole spin qubit" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6156604). *Nature Communications*. **9** (1): 3902. arXiv:1802.00395 (https://arxiv.org/abs/1802.00395). Bibcode:2018NatCo...9.3902W (https://ui.adsabs.harvard.edu/abs/2018NatCo...9.3902W). doi:10.1038/s41467-018-06418-4 (https://doi.org/10.1038%2Fs41467-018-06418-4). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 6156604 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6156604). PMID 30254225 (https://pubmed.ncbi.nlm.nih.gov/30254225).
10. Trauzettel, Björn; Bulaev, Denis V.; Loss, Daniel; Burkard, Guido (2007). "Spin qubits in graphene quantum dots". *Nature Physics*. **3** (3): 192–196. arXiv:cond-mat/0611252 (https://arxiv.org/abs/cond-mat/0611252). Bibcode:2007NatPh...3..192T (https://ui.adsabs.harvard.edu/abs/2007NatPh...3..192T). doi:10.1038/nphys544 (https://doi.org/10.1038%2Fnphys544). ISSN 1745-2473 (https://search.worldcat.org/issn/1745-2473). S2CID 119431314 (https://api.semanticscholar.org/CorpusID:119431314).
11. D. P. DiVincenzo, in Mesoscopic Electron Transport, Vol. 345 of NATO Advanced Study Institute, Series E: Applied Sciences, edited by L. Sohn, L. Kouwenhoven, and G. Schoen (Kluwer, Dordrecht, 1997); on arXiv.org in Dec. 1996 (https://arxiv.org/abs/cond-mat/9612126)
12. Barenco, Adriano; Deutsch, David; Ekert, Artur; Josza, Richard (1995). "Conditional Quantum Dynamics and Logic Gates". *Phys. Rev. Lett*. **74** (20): 4083–4086. arXiv:quant-ph/9503017 (https://arxiv.org/abs/quant-ph/9503017). Bibcode:1995PhRvL..74.4083B (https://ui.adsabs.harvard.edu/abs/1995PhRvL..74.4083B). doi:10.1103/PhysRevLett.74.4083 (https://doi.org/10.1103%2FPhysRevLett.74.4083). PMID 10058408 (https://pubmed.ncbi.nlm.nih.gov/10058408). S2CID 26611140 (https://api.semanticscholar.org/CorpusID:26611140).

External links

- QuantumInspire (https://www.quantum-inspire.com/contact) online platform from Delft University of Technology, allows building and running quantum algorithms on "Spin-2" a 2

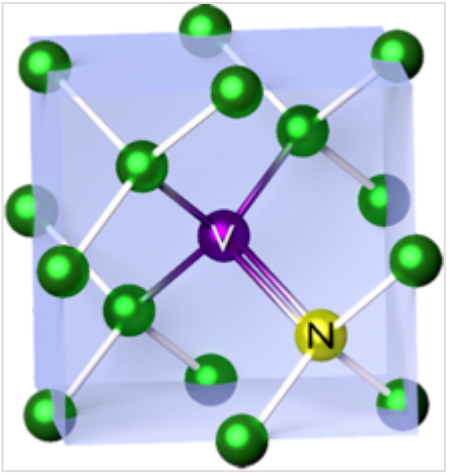
silicon spin qubits processor.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Spin_qubit_quantum_computer&oldid=1230119039"

WIKIPEDIA
The Free Encyclopedia

Nitrogen-vacancy center

The **nitrogen-vacancy center** (**N-V center** or **NV center**) is one of numerous photoluminescent point defects in diamond. Its most explored and useful properties include its spin-dependent photoluminescence (which enables measurement of the electronic spin state using optically detected magnetic resonance), and its relatively long (millisecond) spin coherence at room temperature.[1] The NV center energy levels are modified by magnetic fields,[2] electric fields,[3] temperature,[4] and strain,[5] which allow it to serve as a sensor of a variety of physical phenomena. Its atomic size and spin properties can form the basis for useful quantum sensors.[6] It has also been explored for applications in quantum computing (e.g. for entanglement generation[7]), quantum simulation,[8] and spintronics.[9]



Simplified atomic structure of the NV center

Structure

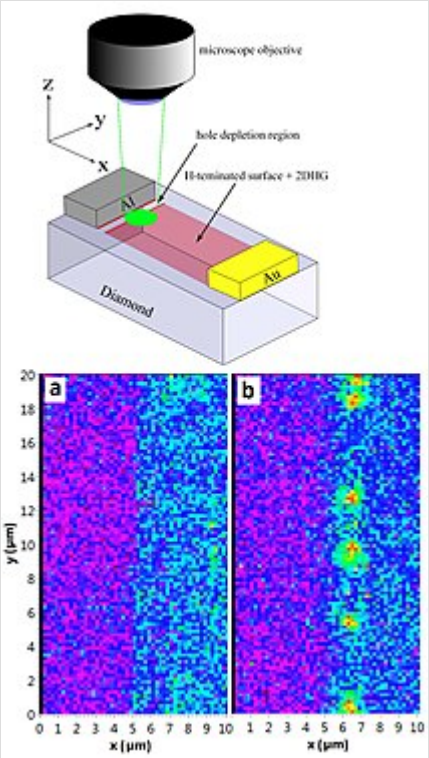
The nitrogen-vacancy center is a point defect in the diamond lattice. It consists of a nearest-neighbor pair of a nitrogen atom, which substitutes for a carbon atom, and a lattice vacancy.

Two charge states of this defect, neutral NV^0 and negative NV^-, are known from spectroscopic studies using optical absorption,[11][12] photoluminescence (PL),[13] electron paramagnetic resonance (EPR)[14][15][16] and optically detected magnetic resonance (ODMR),[17] which can be viewed as a hybrid of PL and EPR; most details of the structure originate from EPR. The nitrogen atom on one hand has five valence electrons. Three of them are covalently bonded to the carbon atoms, while the other two remain non-bonded and are called a lone pair. The vacancy on the other hand has three unpaired electrons. Two of them form a quasi covalent bond and one remains unpaired. The overall symmetry, however, is axial (trigonal C_{3V}); one can visualize this by imagining the three unpaired vacancy electrons continuously exchanging their roles.

The NV^0 thus has one unpaired electron and is paramagnetic. However, despite extensive efforts, electron paramagnetic resonance signals from NV^0 avoided detection for decades until 2008. Optical excitation is required to bring the NV^0 defect into the EPR-detectable excited state; the signals from the ground state are presumably too broad for EPR detection.[18]

The NV^0 centers can be converted into NV^- by changing the Fermi level position. This can be achieved by applying external voltage to a p-n junction made from doped diamond, e.g., in a Schottky diode.[10]

In the negative charge state NV^-, an extra electron is located at the vacancy site forming a spin S=1 pair with one of the vacancy electrons. As in NV^0, the vacancy electrons are "exchanging roles" preserving the overall trigonal symmetry. This NV^- state is what is commonly, and somewhat incorrectly, called "the nitrogen-vacancy center". The neutral state is not generally used for quantum technology.

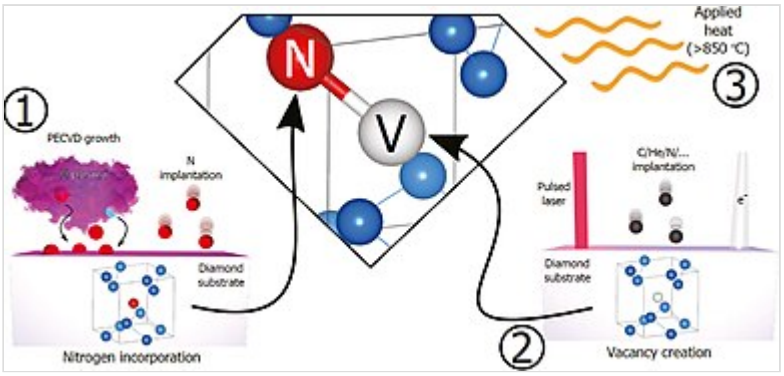


Bottom images are spatial photoluminescence (PL) maps before and after application of +20 V voltage to a planar Schottky diode. The top image outlines the experiment. The PL maps reveal the conversion of individual NV^0 centers into NV^- centers that appear as bright dots.[10]

The NV centers are randomly oriented within a diamond crystal. Ion implantation techniques can enable their artificial creation in predetermined positions.[19]

Production

Nitrogen-vacancy centers are typically produced from single substitutional nitrogen centers (called C or P1 centers in diamond literature) by irradiation followed by annealing at temperatures above 700 °C.[11] A wide range of high-energy particles is suitable for such irradiation, including electrons, protons, neutrons, ions, and gamma photons. Irradiation produces lattice vacancies, which are a part of NV centers. Those vacancies are immobile at room temperature, and annealing is required to move them. Single substitutional nitrogen produces strain in the diamond lattice;[20] it therefore efficiently captures moving vacancies,[21] producing the NV centers.



Production of nitrogen-vacancy centers in diamond may require several steps. First, nitrogen must be introduced into the diamond lattice which can be accomplished via ion implantation or CVD delta doping. Secondly, vacancies must be introduced, which can be accomplished via laser irradiation, ion implantation, or electron irradiation. Alternatively, during the nitrogen introduction step, vacancies may also be introduced. Finally, a high-temperature annealing step can help promote NV formation.[22]

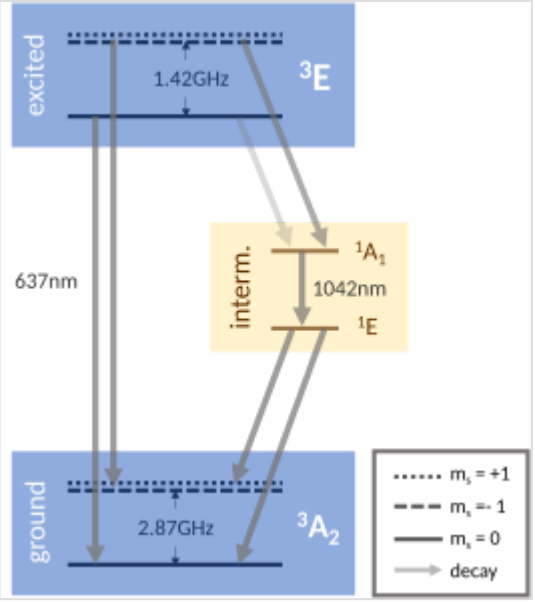
During chemical vapor deposition of diamond, a small fraction of single substitutional nitrogen impurity (typically <0.5%) traps vacancies generated as a result of the plasma synthesis. Such nitrogen-vacancy centers are preferentially aligned to the growth direction.[23][24] Delta doping of nitrogen during CVD growth can be used to create two-dimensional ensembles of NV centers near the diamond surface for enhanced sensing[25] or simulation.[26]

Diamond is notorious for having a relatively large lattice strain. Strain splits and shifts optical transitions from individual centers resulting in broad lines in the ensembles of centers.[11][27] Special care is taken to produce extremely sharp NV lines (line width ~10 MHz)[28] required for most experiments: high-quality, pure natural or better synthetic diamonds (type IIa) are selected. Many of them already have sufficient concentrations of grown-in NV centers and are suitable for applications. If not, they are irradiated by high-energy particles and annealed. Selection of a certain irradiation dose allows tuning the concentration

of produced NV centers such that individual NV centers are separated by micrometre-large distances. Then, individual NV centers can be studied with standard optical microscopes or, better, near-field scanning optical microscopes having sub-micrometre resolution.[17][29]

Energy level structure

The NV center has a **ground-state triplet (^{3}A)**, an **excited-state triplet (^{3}E)** and two **intermediate-state singlets (^{1}A and ^{1}E)**.[note 1][33][34] Both ^{3}A and ^{3}E contain $m_s = \pm 1$ spin states, in which the two electron spins are aligned (either up, such that $m_s = +1$ or down, such that $m_s = -1$), and an $m_s = 0$ spin state where the electron spins are antiparallel. Due to the magnetic interaction, the energy of the $m_s = \pm 1$ states is higher than that of the $m_s = 0$ state. ^{1}A and ^{1}E only contain a spin state singlet each with $m_s = 0$.



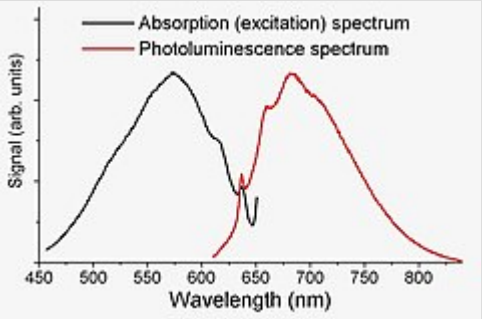
Schematic energy level structure of the NV center. Electron transitions between the ground ^{3}A and excited ^{3}E states, separated by 1.945 eV (637 nm), produce absorption and luminescence. The ^{3}A state is split by 2.87 GHz[30][31] and the ^{3}E state by 1.42 GHz.[32] Numbers 0, ±1 indicate spin quantum number m_s; splitting due to the orbital degeneracy is not shown.

If an external magnetic field is applied along the defect axis (the axis which aligns with the nitrogen atom and the vacancy) of the NV center, it does not affect the $m_s = 0$ states, but it splits the $m_s = \pm 1$ levels (Zeeman effect). Similarly the following other properties of the environment influence the energy level diagram :

1. Amplitude and orientation of a static magnetic field splits the $m_s = \pm 1$ levels in the ground and excited states.
2. Amplitude and orientation of elastic (strain) or electric fields[35][36] have a much smaller but also more complex effects on the different levels.
3. Continuous-wave microwave radiation (applied in resonance with the transition between $m_s = 0$ and (one of the) $m_s = \pm 1$ states) changes the population of the sublevels within the ground and excited state.[36]
4. A tunable laser can selectively excite certain sublevels of the ground and excited states.[36][37]
5. Surrounding spins and spin–orbit interaction will modulate the magnetic field experienced by the NV center.
6. Temperature and pressure affect different parts of the spectrum including the shift between ground and excited states.

The above-described energy structure[note 2] is by no means exceptional for a defect in diamond or other semiconductor.[38] It was not this structure alone, but a combination of several favorable factors (previous knowledge, easy production, biocompatibility, simple initialisation, use at room temperature etc.) which suggested the use of the NV center as a qubit and quantum sensor.

Optical properties



Optical absorption and emission of the NV^- center at room temperature.

NV centers emit bright red light ($^3E \rightarrow {}^3A$ transitions), if excited off-resonantly by visible green light ($^3A \rightarrow {}^3E$ transitions). This can be done with convenient light sources such as argon or krypton lasers, frequency doubled Nd:YAG lasers, dye lasers, or He-Ne lasers. Excitation can also be achieved at energies below that of zero phonon emission.[39]

As the relaxation time from the excited state is small (~10 ns),[40][41] the emission happens almost instantly after the excitation. At room temperature the NV center's optical spectrum exhibits no sharp peaks due to thermal broadening. However, cooling the NV centers with liquid nitrogen or liquid helium dramatically narrows the lines down to a width of a few MHz. At low temperature it also becomes possible to specifically address the zero-phonon line (ZPL).

An important property of the luminescence from individual NV centers is its high temporal stability. Whereas many single-molecular emitters bleach (i.e. change their charge state and become dark) after emission of 10^6–10^8 photons, bleaching is unlikely for NV centers at room temperature.[42][29] Strong laser illumination, however, may also convert some NV^- into NV^0 centers.[13]

Because of these properties, the ideal technique to address the NV centers is confocal microscopy, both at room temperature and at low temperature.

State manipulation

Optical spin manipulation

Optical transitions must preserve the total spin and occur only between levels of the same total spin. Specifically, transitions between the ground and excited states (with equal spin) can be induced using a green laser with a wavelength of 546 nm. Transitions $^3E \rightarrow {}^1A$ and $^1E \rightarrow {}^3A$ are non-radiative, while $^1A \rightarrow {}^1E$ has both a non-radiative and infrared decay path.

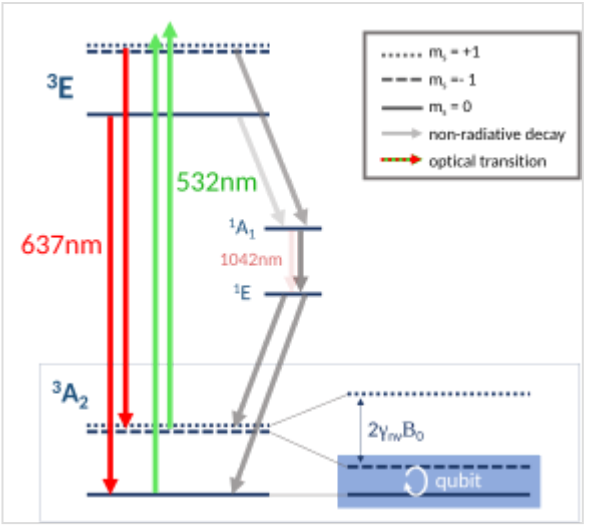
The diagram on the right shows the multi-electronic states of the NV center labeled according to their symmetry (E or A) and their spin state (3 for a triplet (S=1) and 1 for a singlet (S=0)). There are two triplet states and two intermediate singlet states.[47]

Spin-state initialisation

An important property of the non-radiative transition between ^3E and ^1A is that it is stronger for $m_s = \pm 1$ and weaker for $m_s = 0$. This provides the basis a very useful manipulation strategy, which is called spin state initialisation (or optical spin-polarization). To understand the process, first consider an off-resonance excitation which has a higher frequency (typically 2.32 eV (532 nm)) than the frequencies of all transitions and thus lies in the vibronic bands for all transitions. By using a pulse of this wavelength, one can excite all spin states from ^3A to ^3E. An NV center in the ground state with $m_s = 0$ will be excited to the corresponding excited state with $m_s = 0$ due to the conservation of spin. Afterwards it decays back to its original state. For a ground state with $m_s = \pm 1$, the situation is different. After the excitation, it has a

relatively high probability to decay into the intermediate state ^1A by non-radiative transition[note 3][48] and further into the ground state with $m_s = 0$. After many cycles, the state of the NV center (independently of whether it started in $m_s = 0$ or $m_s = \pm 1$) will end up in the $m_s = 0$ ground state. This process can be used to initialize the quantum state of a qubit for quantum information processing or quantum sensing.

Sometimes the polarisability of the NV center is explained by the claim that the transition from ^1E to the ground state with $m_s = \pm 1$ is small, compared to the transition to $m_s = 0$. However, it has been shown that the comparatively low decay probability for $m_s = 0$ states w.r.t. $m_s = \pm 1$ states into ^1A is enough to explain the polarization.[49]



Spin dynamics in the NV center in diamond. The primary transition between the ground and excited state triplets is spin conserving. Decay via the intermediate singlets gives rise to spin polarization by converting spin from $m_s = \pm 1$ to $m_s = 0$. Both absorption and emission wavelengths are indicated,[43] since they differ due to Stokes shift.[44][45] Furthermore, the effect of a static magnetic field B_0 along the defect axis and the resulting Zeeman shift is indicated. Here, γ_{nv} refers to the gyromagnetic ratio of the NV center. In many applications two of the ground-state levels are then used as a qubit.[46] Transitions in this effective two-level system, may be induced using a microwave field. 3E-1A and 1E-3A are non-radiative transitions.

Effects of external fields

Microwave spin manipulation

The energy difference between the $m_s = 0$ and $m_s = \pm 1$ states corresponds to the microwave regime. Population can be transferred between the states by applying a resonant magnetic field perpendicular to the defect axis. Numerous dynamic effects (spin echo, Rabi oscillations, etc.) can be exploited by applying a carefully designed sequence of microwave pulses.[50][51][52][53][54] Such protocols are rather important for the practical realization of quantum computers. By manipulating the population, it is possible to shift the NV center into a more sensitive or stable state.[55][56] Its own resulting fluctuating fields may also be used to influence the surrounding nuclei[57] or protect the NV center itself from noise.[58] This is typically done using a wire loop (microwave antenna) which creates an oscillating magnetic field.[59]

Influence of external factors

If a **magnetic field** is oriented along the defect axis it leads to Zeeman splitting separating the $m_s = +1$ from the $m_s = -1$ states. This technique is used to lift the degeneracy and use only two of the spin states (usually the ground states with $m_s = -1$ and $m_s = 0$) as a qubit. Population can then be transferred between them using a microwave field. In the specific instance that the magnetic field reaches 1027 G (or 508 G) then the $m_s = -1$ and $m_s = 0$ states in the ground (or excited) state become equal in energy (Ground/Excited State Level Anticrossing). The following strong interaction results in so-called spin polarization, which strongly affects the intensity of optical absorption and luminescence transitions involving those states.[32]

Importantly, this splitting can be modulated by applying an **external electric field**,[35][36] in a similar fashion to the magnetic field mechanism outlined above, though the physics of the splitting is somewhat more complex. Nevertheless, an important practical outcome is that the intensity and position of the luminescence lines is modulated. **Strain** has a similar effect on the NV center as electric fields.[60]

There is an additional splitting of the $m_s = \pm 1$ energy levels, which originates from the hyperfine interaction between surrounding **nuclear spins** and the NV center. These nuclear spins create magnetic and electric fields of their own leading to further distortions of the NV spectrum (see nuclear Zeeman and quadrupole interaction). Also the NV center's own spin–orbit interaction and orbital degeneracy leads to additional level splitting in the excited ^{3}E state.

Temperature and **pressure** directly influence the zero-field term of the NV center leading to a shift between the ground and excited state levels.

The Hamiltonian, a quantum mechanical equation describing the dynamics of a system, which shows the influence of different factors on the NV center can be found below.

$$\hat{H} = \overbrace{\hbar D\left[\hat{S}_Z^2 - \frac{2}{3}\right] + \hbar E(\hat{S}_X^2 - \hat{S}_Y^2)}^{\text{zero-field term}} + \overbrace{\hbar\gamma_{nv}\vec{B}\cdot\hat{\vec{S}}}^{\text{magnetic interaction}} + \overbrace{\hbar\delta_{\parallel}\mathcal{E}_Z\left[\hat{S}_Z^2 - \frac{2}{3}\right] - \hbar\delta_{\perp}\left[\mathcal{E}_X(\hat{S}_X\hat{S}_Y + \hat{S}_Y\hat{S}_X) + \mathcal{E}_Y(\hat{S}_X^2 - \hat{S}_Y^2)\right]}^{\text{electric interaction}}$$
$$+\hbar\sum_{i=1}^{n}\left(\underbrace{\hat{\vec{S}}\mathcal{N}_i\hat{\vec{I}}_i}_{\text{hyperfine interaction}} + \underbrace{\gamma_i\vec{B}\cdot\hat{\vec{I}}_i}_{\text{nuclear Zeeman interaction}} + \underbrace{Q_i\hat{I}_{Z,i}^2}_{\text{nuclear quadrupole interaction}}\right)$$

Although it can be challenging, all of these effects are measurable, making the NV center a perfect candidate for a quantum sensor.[56]

Charge state manipulation

It is also possible to switch the charge state of the NV center (i.e. between NV^-, NV^+ and NV^0) by applying a gate voltage.[61]

Applications

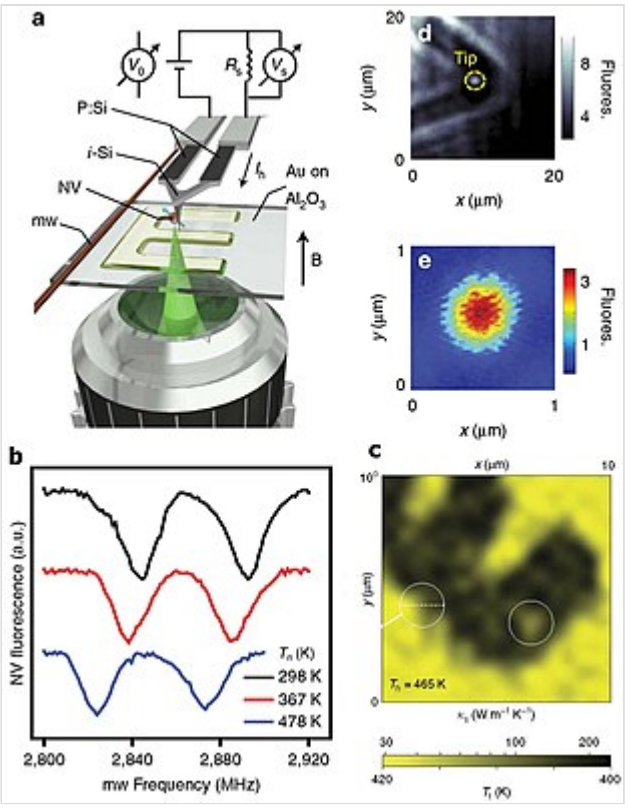
The spectral shape and intensity of the optical signals from the NV^- centers are sensitive to external perturbation, such as temperature, strain, electric and magnetic field. However, the use of spectral shape for sensing those perturbation is impractical, as the diamond would have to be cooled to cryogenic temperatures to sharpen the NV^- signals. A more realistic approach is to use luminescence intensity (rather than lineshape), which exhibits a sharp resonance when a microwave frequency is applied to diamond that matches the splitting of the ground-state levels. The resulting optically detected magnetic resonance signals are sharp even at room temperature, and can be used in miniature sensors. Such sensors can detect magnetic fields of a few nanotesla[63] or electric fields of about 10 V/cm[64] at kilohertz frequencies after 100 seconds of averaging. This sensitivity allows detecting a magnetic or electric field produced by a single electron located tens of nanometers away from an NV^- center.

Using the same mechanism, the NV^- centers were employed in scanning thermal microscopy to measure high-resolution spatial maps of temperature and thermal conductivity (see image).[62]

Because the NV center is sensitive to magnetic fields, it is being actively used in scanning probe measurements to study myriad condensed matter phenomena both through measuring a spatially varying magnetic field or inferring local currents in a device.[65][66][67][68][69]

Another possible use of the NV^- centers is as a detector to measure the full mechanical stress tensor in the bulk of the crystal. For this application, the stress-induced splitting of the zero-phonon-line is exploited, and its polarization properties.[70] A robust frequency-modulated radio receiver using the electron-spin-dependent photoluminescence that operated up to 350 °C demonstrates the possibility for use in extreme conditions.[71]

In addition to the quantum optical applications, luminescence from the NV^- centers can be applied for imaging biological processes, such as fluid flow in living cells.[72][73] This application relies on good compatibility of diamond nano-particles with the living cells and on favorable properties of photoluminescence from the NV^- centers (strong intensity, easy excitation and detection, temporal stability, etc.). Compared with large single-crystal diamonds, nanodiamonds are cheap (about 1 USD per gram) and available from various suppliers. NV^- centers are produced in diamond powders with sub-micrometre particle size using the standard process of irradiation and annealing described above. Due to the relatively small size of nanodiamond, NV centers can be produced by irradiating nanodiamond of 100 nm or less with medium energy H+ beam. This method reduces the required ion dose and reaction, making it possible to mass produce fluorescent nanodiamonds in ordinary laboratory.[74] Fluorescent nanodiamond produced with such method is bright and photostable, making it excellent for long-term, three dimensional tracking of single particle in living cell.[75] Those nanodiamonds are introduced in a cell, and their luminescence is monitored using a standard fluorescence microscope.[76]



Scanning thermal microscopy using the NV center. (a) Schematics of experimental setup. An electric current is applied to the arms of an AFM cantilever (phosphorus-doped Si, P:Si) and heats up the end section above the tip (intrinsic Si, *i*-Si). The bottom lens excites a diamond nanocrystal with a green laser light and collects photoluminescence (PL). The crystal hosts an NV center and is attached to the AFM tip. A wire on the sample surface serves as the microwave source (mw). The temperature of the cantilever T_h is determined from the applied current and voltage.
(b) ODMR spectra of the NV center at three temperatures. The line splitting originates from a ~1 mT applied magnetic field.
(c) Thermal conductivity image of a gold letter E on sapphire. White circles indicate features that do not correlate with the AFM topography. (d) PL image of the AFM cantilever end and tip where the diamond nanocrystal appears as the bright spot. (e) Zoomed PL image of the NV center in d.[62]

Stimulated emission from the NV^- center has been demonstrated, though it could be achieved only from the phonon side-band (i.e. broadband light) and not from the ZPL. For this purpose, the center has to be excited at a wavelength longer than ~650 nm, as higher-energy excitation ionizes the center.[77]

The first continuous-wave room-temperature maser has been demonstrated.[78][79] It used 532-nm pumped NV^- centers held within a high Purcell factor microwave cavity and an external magnetic field of 4300 G. Continuous maser oscillation generated a coherent signal at ~9.2 GHz.

The NV center can have a very long spin coherence time approaching the second regime.[80] This is advantageous for applications in quantum sensing[81] and quantum communication.[82] Disadvantageous for these applications is the long radiative lifetime (~12 ns[83][84]) of the NV center and the strong phonon sideband in its emission spectrum. Both issues can be addressed by putting the NV center in an optical cavity.[85]

Historical remarks

The microscopic model and most optical properties of ensembles of the NV^- centers have been firmly established in the 1970s based on the optical measurements combined with uniaxial stress[11] and on the electron paramagnetic resonance.[14][15] However, a minor error in EPR results (it was assumed that illumination is required to observe NV^- EPR signals) resulted in the incorrect multiplicity assignments in the energy level structure. In 1991 it was shown that EPR can be observed without illumination,[16] which established the energy level scheme shown above. The magnetic splitting in the excited state has been measured only recently.[32]

The characterization of single NV^- centers has become a very competitive field nowadays, with many dozens of papers published in the most prestigious scientific journals. One of the first results was reported back in 1997.[17] In that paper, it was demonstrated that the fluorescence of single NV^- centers can be detected by room-temperature fluorescence microscopy and that the defect shows perfect photostability. Also one of the outstanding properties of the NV center was demonstrated, namely room-temperature optically detected magnetic resonance.

See also

- Crystallographic defects in diamond
- Crystallographic defect
- Material properties of diamond

Notes

1. Group theory results are used to take into account the symmetry of the diamond crystal, and so the symmetry of the NV itself. Followingly, the energy levels are labeled according to group theory, and in particular are labelled after the irreducible representations of the C_{3V} symmetry group of the defect center, A_1, A_2, and E. The "3" in $^3A_2$ and ^3E as well as the "1" in $^1A_1$ and ^1E represent the number of allowable m_s spin states, or the spin multiplicity, which range from $-S$ to S for a total of $2S+1$ possible states. If $S = 1$, m_s can be −1, 0, or 1.
2. The energy level structure of the NV center was established by combining optically detected magnetic resonance (ODMR), electron paramagnetic resonance (EPR) and theoretical results, as shown in the figure. In particular, several theoretical works have been done,

using the Linear Combination of Atomic Orbitals (LCAO) approach, to build the electronic orbitals to describe the possible quantum states, looking at the NV center as a molecule.

3. This is a phenomenon called intersystem crossing (ISC). It happens at an appreciable rate because the energy curve in function of the position of the atoms for the excited $m_S = \pm 1$ state intersects the curve for the ^1A state. Therefore, for some instant during the vibrational relaxation that the ions undergo after the excitement, it is possible for the spin to flip with little or no energy required in the transition.

References

1. Hanson, R.; Gywat, O.; Awschalom, D. D. (2006-10-26). "Room-temperature manipulation and decoherence of a single spin in diamond" (https://link.aps.org/doi/10.1103/PhysRevB.74.161203). *Physical Review B*. **74** (16): 161203. arXiv:quant-ph/0608233 (https://arxiv.org/abs/quant-ph/0608233). Bibcode:2006PhRvB..74p1203H (https://ui.adsabs.harvard.edu/abs/2006PhRvB..74p1203H). doi:10.1103/PhysRevB.74.161203 (https://doi.org/10.1103%2FPhysRevB.74.161203). S2CID 5055366 (https://api.semanticscholar.org/CorpusID:5055366).
2. Maze, J. R.; Stanwix, P. L.; Hodges, J. S.; Hong, S.; Taylor, J. M.; Cappellaro, P.; Jiang, L.; Dutt, M. V. Gurudev; Togan, E.; Zibrov, A. S.; Yacoby, A.; Walsworth, R. L.; Lukin, M. D. (October 2008). "Nanoscale magnetic sensing with an individual electronic spin in diamond" (https://www.nature.com/articles/nature07279). *Nature*. **455** (7213): 644–647. Bibcode:2008Natur.455..644M (https://ui.adsabs.harvard.edu/abs/2008Natur.455..644M). doi:10.1038/nature07279 (https://doi.org/10.1038%2Fnature07279). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 18833275 (https://pubmed.ncbi.nlm.nih.gov/18833275).
3. Dolde, F.; Fedder, H.; Doherty, M. W.; Nöbauer, T.; Rempp, F.; Balasubramanian, G.; Wolf, T.; Reinhard, F.; Hollenberg, L. C. L.; Jelezko, F.; Wrachtrup, J. (June 2011). "Electric-field sensing using single diamond spins" (https://doi.org/10.1038%2Fnphys1969). *Nature Physics*. **7** (6): 459–463. arXiv:1103.3432 (https://arxiv.org/abs/1103.3432). Bibcode:2011NatPh...7..459D (https://ui.adsabs.harvard.edu/abs/2011NatPh...7..459D). doi:10.1038/nphys1969 (https://doi.org/10.1038%2Fnphys1969). hdl:11858/00-001M-0000-0027-768E-1 (https://hdl.handle.net/11858%2F00-001M-0000-0027-768E-1). ISSN 1745-2481 (https://search.worldcat.org/issn/1745-2481). S2CID 119287960 (https://api.semanticscholar.org/CorpusID:119287960).
4. Kucsko, G.; Maurer, P. C.; Yao, N. Y.; Kubo, M.; Noh, H. J.; Lo, P. K.; Park, H.; Lukin, M. D. (August 2013). "Nanometre-scale thermometry in a living cell" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4221854). *Nature*. **500** (7460): 54–58. arXiv:1304.1068 (https://arxiv.org/abs/1304.1068). Bibcode:2013Natur.500...54K (https://ui.adsabs.harvard.edu/abs/2013Natur.500...54K). doi:10.1038/nature12373 (https://doi.org/10.1038%2Fnature12373). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 4221854 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4221854). PMID 23903748 (https://pubmed.ncbi.nlm.nih.gov/23903748).
5. Maze, J R; Gali, A; Togan, E; Chu, Y; Trifonov, A; Kaxiras, E; Lukin, M D (2011-02-28). "Properties of nitrogen-vacancy centers in diamond: the group theoretic approach" (https://iopscience.iop.org/article/10.1088/1367-2630/13/2/025025). *New Journal of Physics*. **13** (2): 025025. arXiv:1010.1338 (https://arxiv.org/abs/1010.1338). Bibcode:2011NJPh...13b5025M (https://ui.adsabs.harvard.edu/abs/2011NJPh...13b5025M). doi:10.1088/1367-2630/13/2/025025 (https://doi.org/10.1088%2F1367-2630%2F13%2F2%2F025025). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 16820460 (https://api.semanticscholar.org/CorpusID:16820460).

6. Degen, C. L.; Reinhard, F.; Cappellaro, P. (2017-07-25). "Quantum sensing" (https://doi.org/10.1103%2FRevModPhys.89.035002). *Reviews of Modern Physics*. **89** (3): 035002. arXiv:1611.02427 (https://arxiv.org/abs/1611.02427). Bibcode:2017RvMP...89c5002D (https://ui.adsabs.harvard.edu/abs/2017RvMP...89c5002D). doi:10.1103/RevModPhys.89.035002 (https://doi.org/10.1103%2FRevModPhys.89.035002). hdl:1721.1/124553 (https://hdl.handle.net/1721.1%2F124553). S2CID 2555443 (https://api.semanticscholar.org/CorpusID:2555443).
7. Bernien, H.; Hensen, B.; Pfaff, W.; Koolstra, G.; Blok, M. S.; Robledo, L.; Taminiau, T. H.; Markham, M.; Twitchen, D. J.; Childress, L.; Hanson, R. (May 2013). "Heralded entanglement between solid-state qubits separated by three metres" (https://www.nature.com/articles/nature12016). *Nature*. **497** (7447): 86–90. arXiv:1212.6136 (https://arxiv.org/abs/1212.6136). Bibcode:2013Natur.497...86B (https://ui.adsabs.harvard.edu/abs/2013Natur.497...86B). doi:10.1038/nature12016 (https://doi.org/10.1038%2Fnature12016). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMID 23615617 (https://pubmed.ncbi.nlm.nih.gov/23615617). S2CID 4383784 (https://api.semanticscholar.org/CorpusID:4383784).
8. Choi, Soonwon; Choi, Joonhee; Landig, Renate; Kucsko, Georg; Zhou, Hengyun; Isoya, Junichi; Jelezko, Fedor; Onoda, Shinobu; Sumiya, Hitoshi; Khemani, Vedika; von Keyserlingk, Curt; Yao, Norman Y.; Demler, Eugene; Lukin, Mikhail D. (March 2017). "Observation of discrete time-crystalline order in a disordered dipolar many-body system" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5349499). *Nature*. **543** (7644): 221–225. doi:10.1038/nature21426 (https://doi.org/10.1038%2Fnature21426). ISSN 1476-4687 (https://search.worldcat.org/issn/1476-4687). PMC 5349499 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5349499). PMID 28277511 (https://pubmed.ncbi.nlm.nih.gov/28277511).
9. Awschalom, David D.; Bassett, Lee C.; Dzurak, Andrew S.; Hu, Evelyn L.; Petta, Jason R. (2013-03-08). "Quantum Spintronics: Engineering and Manipulating Atom-Like Spins in Semiconductors" (https://www.science.org/doi/10.1126/science.1231364). *Science*. **339** (6124): 1174–1179. Bibcode:2013Sci...339.1174A (https://ui.adsabs.harvard.edu/abs/2013Sci...339.1174A). doi:10.1126/science.1231364 (https://doi.org/10.1126%2Fscience.1231364). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 23471400 (https://pubmed.ncbi.nlm.nih.gov/23471400). S2CID 206545890 (https://api.semanticscholar.org/CorpusID:206545890).
10. Schreyvogel, C.; Polyakov, V.; Wunderlich, R.; Meijer, J.; Nebel, C. E. (2015). "Active charge state control of single N-V centres in diamond by in-plane Al-Schottky junctions" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4503995). *Scientific Reports*. **5**: 12160. Bibcode:2015NatSR...512160S (https://ui.adsabs.harvard.edu/abs/2015NatSR...512160S). doi:10.1038/srep12160 (https://doi.org/10.1038%2Fsrep12160). PMC 4503995 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4503995). PMID 26177799 (https://pubmed.ncbi.nlm.nih.gov/26177799).
11. Davies, G.; Hamer, M. F. (1976). "Optical Studies of the 1.945 eV Vibronic Band in Diamond". *Proceedings of the Royal Society of London A*. **348** (1653): 285. Bibcode:1976RSPSA.348..285D (https://ui.adsabs.harvard.edu/abs/1976RSPSA.348..285D). doi:10.1098/rspa.1976.0039 (https://doi.org/10.1098%2Frspa.1976.0039). S2CID 93303167 (https://api.semanticscholar.org/CorpusID:93303167).
12. Mita, Y. (1996). "Change of absorption spectra in type-Ib diamond with heavy neutron irradiation". *Physical Review B*. **53** (17): 11360–11364. Bibcode:1996PhRvB..5311360M (https://ui.adsabs.harvard.edu/abs/1996PhRvB..5311360M). doi:10.1103/PhysRevB.53.11360 (https://doi.org/10.1103%2FPhysRevB.53.11360). PMID 9982752 (https://pubmed.ncbi.nlm.nih.gov/9982752).
13. Iakoubovskii, K.; Adriaenssens, G. J.; Nesladek, M. (2000). "Photochromism of vacancy-related centres in diamond" (http://pubman.nims.go.jp/pubman/item/escidoc:1587366:1/component/escidoc:1587365/jpc189.pdf) (PDF). *Journal of Physics: Condensed Matter*. **12** (2): 189. Bibcode:2000JPCM...12..189I (https://ui.adsabs.harvard.edu/abs/2000JPCM...12..189I). doi:10.1088/0953-8984/12/2/308 (https://doi.org/10.1088%2F0953-8984%2F12%2F2%2F308). S2CID 250820432 (https://api.semanticscholar.org/CorpusID:250820432).

14. Loubser, J. H. N.; van Wyk, J. A. (1977). "Electron Spin Resonance in Annealed Type 1b Diamond". *Diamond Research*. **11**: 4–7. ISSN 0070-4679 (https://search.worldcat.org/issn/0070-4679).
15. Loubser, J. H. N.; van Wyk, J. A. (1978). "Electron spin resonance in the study of diamond". *Reports on Progress in Physics*. **41** (8): 1201. Bibcode:1978RPPh...41.1201L (https://ui.adsabs.harvard.edu/abs/1978RPPh...41.1201L). doi:10.1088/0034-4885/41/8/002 (https://doi.org/10.1088%2F0034-4885%2F41%2F8%2F002). S2CID 250898303 (https://api.semanticscholar.org/CorpusID:250898303).
16. Redman, D.; Brown, S.; Sands, R.; Rand, S. (1991). "Spin dynamics and electronic states of N-V centers in diamond by EPR and four-wave-mixing spectroscopy". *Physical Review Letters*. **67** (24): 3420–3423. Bibcode:1991PhRvL..67.3420R (https://ui.adsabs.harvard.edu/abs/1991PhRvL..67.3420R). doi:10.1103/PhysRevLett.67.3420 (https://doi.org/10.1103%2FPhysRevLett.67.3420). PMID 10044729 (https://pubmed.ncbi.nlm.nih.gov/10044729).
17. Gruber, A.; et al. (1997). "Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers" (http://sites.fas.harvard.edu/~phys191r/References/d4/Gruber1997.pdf) (PDF). *Science*. **276** (5321): 2012–2014. doi:10.1126/science.276.5321.2012 (https://doi.org/10.1126%2Fscience.276.5321.2012).
18. Felton, S.; et al. (2008). "Electron paramagnetic resonance studies of the neutral nitrogen vacancy in diamond" (https://pure.qub.ac.uk/portal/en/publications/electron-paramagnetic-resonance-studies-of-the-neutral-nitrogen-vacancy-in-diamond(c2c09f0e-632f-4687-9fb9-e7085ef7f1c9).html). *Physical Review B*. **77** (8): 081201. Bibcode:2008PhRvB..77h1201F (https://ui.adsabs.harvard.edu/abs/2008PhRvB..77h1201F). doi:10.1103/PhysRevB.77.081201 (https://doi.org/10.1103%2FPhysRevB.77.081201). S2CID 122354274 (https://api.semanticscholar.org/CorpusID:122354274).
19. Awschalom, D. D.; Epstein, R.; Hanson, R. (2007). "Diamond Age of Spintronics". *Scientific American*. **297** (4): 84–91. Bibcode:2007SciAm.297d..84A (https://ui.adsabs.harvard.edu/abs/2007SciAm.297d..84A). doi:10.1038/scientificamerican1007-84 (https://doi.org/10.1038%2Fscientificamerican1007-84). PMID 17926759 (https://pubmed.ncbi.nlm.nih.gov/17926759).
20. Lang, A. R.; et al. (1991). "On the Dilatation of Synthetic Type Ib Diamond by Substitutional Nitrogen Impurity". *Philosophical Transactions of the Royal Society A*. **337** (1648): 497–520. Bibcode:1991RSPTA.337..497L (https://ui.adsabs.harvard.edu/abs/1991RSPTA.337..497L). doi:10.1098/rsta.1991.0135 (https://doi.org/10.1098%2Frsta.1991.0135). S2CID 54190787 (https://api.semanticscholar.org/CorpusID:54190787).
21. Iakoubovskii, K.; Adriaenssens, G. J. (2001). "Trapping of vacancies by defects in diamond" (https://www.researchgate.net/publication/230912003). *Journal of Physics: Condensed Matter*. **13** (26): 6015. Bibcode:2001JPCM...13.6015I (https://ui.adsabs.harvard.edu/abs/2001JPCM...13.6015I). doi:10.1088/0953-8984/13/26/316 (https://doi.org/10.1088%2F0953-8984%2F13%2F26%2F316). S2CID 250804678 (https://api.semanticscholar.org/CorpusID:250804678).
22. Smith, Jason M.; Meynell, Simon A.; Jayich, Ania C. Bleszynski; Meijer, Jan (2019-11-01). "Colour centre generation in diamond for quantum technologies" (https://doi.org/10.1515%2Fnanoph-2019-0196). *Nanophotonics*. **8** (11): 1889–1906. Bibcode:2019Nanop...8..196S (https://ui.adsabs.harvard.edu/abs/2019Nanop...8..196S). doi:10.1515/nanoph-2019-0196 (https://doi.org/10.1515%2Fnanoph-2019-0196). ISSN 2192-8614 (https://search.worldcat.org/issn/2192-8614). S2CID 207968005 (https://api.semanticscholar.org/CorpusID:207968005).
23. Edmonds, A.; d'Haenens-Johansson, U.; Cruddace, R.; Newton, M.; Fu, K. -M.; Santori, C.; Beausoleil, R.; Twitchen, D.; Markham, M. (2012). "Production of oriented nitrogen-vacancy color centers in synthetic diamond". *Physical Review B*. **86** (3): 035201. arXiv:1112.5757 (https://arxiv.org/abs/1112.5757). Bibcode:2012PhRvB..86c5201E (https://ui.adsabs.harvard.edu/abs/2012PhRvB..86c5201E). doi:10.1103/PhysRevB.86.035201 (https://doi.org/10.1103%2FPhysRevB.86.035201). S2CID 118609894 (https://api.semanticscholar.org/CorpusID:118609894).

24. Pham, L. M.; Bar-Gill, N.; Le Sage, D.; Belthangady, C.; Stacey, A.; Markham, M.; Twitchen, D. J.; Lukin, M. D.; Walsworth, R. L. (2012-09-06). "Enhanced metrology using preferential orientation of nitrogen-vacancy centers in diamond" (https://link.aps.org/doi/10.1103/PhysRevB.86.121202). *Physical Review B*. **86** (12): 121202. arXiv:1207.3363 (https://arxiv.org/abs/1207.3363). Bibcode:2012PhRvB..86l1202P (https://ui.adsabs.harvard.edu/abs/2012PhRvB..86l1202P). doi:10.1103/PhysRevB.86.121202 (https://doi.org/10.1103%2FPhysRevB.86.121202). S2CID 3283919 (https://api.semanticscholar.org/CorpusID:3283919).
25. Hughes, Lillian B.; Zhang, Zhiran; Jin, Chang; Meynell, Simon A.; Ye, Bingtian; Wu, Weijie; Wang, Zilin; Davis, Emily J.; Mates, Thomas E.; Yao, Norman Y.; Mukherjee, Kunal; Bleszynski Jayich, Ania C. (2023-02-01). "Two-dimensional spin systems in PECVD-grown diamond with tunable density and long coherence for enhanced quantum sensing and simulation" (https://doi.org/10.1063/5.0133501). *APL Materials*. **11** (2): 021101. arXiv:2211.02282 (https://arxiv.org/abs/2211.02282). Bibcode:2023APLM...11b1101H (https://ui.adsabs.harvard.edu/abs/2023APLM...11b1101H). doi:10.1063/5.0133501 (https://doi.org/10.1063%2F5.0133501). ISSN 2166-532X (https://search.worldcat.org/issn/2166-532X). S2CID 253370730 (https://api.semanticscholar.org/CorpusID:253370730).
26. Davis, E. J.; Ye, B.; Machado, F.; Meynell, S. A.; Wu, W.; Mittiga, T.; Schenken, W.; Joos, M.; Kobrin, B.; Lyu, Y.; Wang, Z.; Bluvstein, D.; Choi, S.; Zu, C.; Jayich, A. C. Bleszynski (June 2023). "Probing many-body dynamics in a two-dimensional dipolar spin ensemble" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10264245). *Nature Physics*. **19** (6): 836–844. Bibcode:2023NatPh..19..836D (https://ui.adsabs.harvard.edu/abs/2023NatPh..19..836D). doi:10.1038/s41567-023-01944-5 (https://doi.org/10.1038%2Fs41567-023-01944-5). ISSN 1745-2481 (https://search.worldcat.org/issn/1745-2481). PMC 10264245 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10264245). PMID 37323805 (https://pubmed.ncbi.nlm.nih.gov/37323805).
27. *Quantum Information Processing with Diamond* (https://linkinghub.elsevier.com/retrieve/pii/C20130163295). Elsevier. 2014. doi:10.1016/c2013-0-16329-5 (https://doi.org/10.1016%2Fc2013-0-16329-5). ISBN 978-0-85709-656-2. S2CID 119422670 (https://api.semanticscholar.org/CorpusID:119422670).
28. Tamarat, Ph.; et al. (2006). "Stark Shift Control of Single Optical Centers in Diamond". *Physical Review Letters*. **97** (8): 083002. arXiv:quant-ph/0607170 (https://arxiv.org/abs/quant-ph/0607170). Bibcode:2006PhRvL..97h3002T (https://ui.adsabs.harvard.edu/abs/2006PhRvL..97h3002T). doi:10.1103/PhysRevLett.97.083002 (https://doi.org/10.1103%2FPhysRevLett.97.083002). PMID 17026299 (https://pubmed.ncbi.nlm.nih.gov/17026299). S2CID 33870769 (https://api.semanticscholar.org/CorpusID:33870769).
29. Kuhn, S.; et al. (2001). "Diamond colour centres as a nanoscopic light source for scanning near-field optical microscopy". *Journal of Microscopy*. **202** (1): 2–6. doi:10.1046/j.1365-2818.2001.00829.x (https://doi.org/10.1046%2Fj.1365-2818.2001.00829.x). PMID 11298860 (https://pubmed.ncbi.nlm.nih.gov/11298860). S2CID 26077916 (https://api.semanticscholar.org/CorpusID:26077916).
30. Loubser, J. H. N.; van Wyk, J. A. (1977). "Electron Spin Resonance in Annealed Type 1b Diamond". *Diamond Research*. **11**: 4–7. ISSN 0070-4679 (https://search.worldcat.org/issn/0070-4679).
31. Loubser, J. H. N.; van Wyk, J. A. (1978). "Electron spin resonance in the study of diamond". *Reports on Progress in Physics*. **41** (8): 1201. Bibcode:1978RPPh...41.1201L (https://ui.adsabs.harvard.edu/abs/1978RPPh...41.1201L). doi:10.1088/0034-4885/41/8/002 (https://doi.org/10.1088%2F0034-4885%2F41%2F8%2F002). S2CID 250898303 (https://api.semanticscholar.org/CorpusID:250898303).

32. Fuchs, G. D.; et al. (2008). "Excited-State Spectroscopy Using Single Spin Manipulation in Diamond". *Physical Review Letters*. **101** (1): 117601. arXiv:0806.1939 (https://arxiv.org/abs/0806.1939). Bibcode:2008PhRvL.101k7601F (https://ui.adsabs.harvard.edu/abs/2008PhRvL.101k7601F). doi:10.1103/PhysRevLett.101.117601 (https://doi.org/10.1103%2FPhysRevLett.101.117601). PMID 18851332 (https://pubmed.ncbi.nlm.nih.gov/18851332). S2CID 24822943 (https://api.semanticscholar.org/CorpusID:24822943).
33. Manson, N. B.; Harrison, J. P.; Sellars, M. J. (2006-09-21). "Nitrogen-vacancy center in diamond: Model of the electronic structure and associated dynamics". *Physical Review B*. **74** (10): 104303. arXiv:cond-mat/0601360 (https://arxiv.org/abs/cond-mat/0601360). Bibcode:2006PhRvB..74j4303M (https://ui.adsabs.harvard.edu/abs/2006PhRvB..74j4303M). doi:10.1103/PhysRevB.74.104303 (https://doi.org/10.1103%2FPhysRevB.74.104303).
34. Gali, Ádám (2019-11-01). "Ab initio theory of the nitrogen-vacancy center in diamond". *Nanophotonics*. **8** (11): 1907–1943. arXiv:1906.00047 (https://arxiv.org/abs/1906.00047). Bibcode:2019Nanop...8..154G (https://ui.adsabs.harvard.edu/abs/2019Nanop...8..154G). doi:10.1515/nanoph-2019-0154 (https://doi.org/10.1515%2Fnanoph-2019-0154). S2CID 202236167 (https://api.semanticscholar.org/CorpusID:202236167).
35. Tamarat, Ph.; et al. (2006). "Stark Shift Control of Single Optical Centers in Diamond". *Physical Review Letters*. **97** (8): 083002. arXiv:quant-ph/0607170 (https://arxiv.org/abs/quant-ph/0607170). Bibcode:2006PhRvL..97h3002T (https://ui.adsabs.harvard.edu/abs/2006PhRvL..97h3002T). doi:10.1103/PhysRevLett.97.083002 (https://doi.org/10.1103%2FPhysRevLett.97.083002). PMID 17026299 (https://pubmed.ncbi.nlm.nih.gov/17026299). S2CID 33870769 (https://api.semanticscholar.org/CorpusID:33870769).
36. Tamarat, Ph.; et al. (2008). "Spin-flip and spin-conserving optical transitions of the nitrogen-vacancy centre in diamond" (https://doi.org/10.1088%2F1367-2630%2F10%2F4%2F045004). *New Journal of Physics*. **10** (4): 045004. Bibcode:2008NJPh...10d5004T (https://ui.adsabs.harvard.edu/abs/2008NJPh...10d5004T). doi:10.1088/1367-2630/10/4/045004 (https://doi.org/10.1088%2F1367-2630%2F10%2F4%2F045004). hdl:1969.1/179402 (https://hdl.handle.net/1969.1%2F179402). S2CID 37554428 (https://api.semanticscholar.org/CorpusID:37554428).
37. Santori, C.; et al. (2006). "Coherent Population Trapping of Single Spins in Diamond under Optical Excitation". *Physical Review Letters*. **97** (24): 247401. arXiv:quant-ph/0607147 (https://arxiv.org/abs/quant-ph/0607147). Bibcode:2006PhRvL..97x7401S (https://ui.adsabs.harvard.edu/abs/2006PhRvL..97x7401S). doi:10.1103/PhysRevLett.97.247401 (https://doi.org/10.1103%2FPhysRevLett.97.247401). hdl:2318/103560 (https://hdl.handle.net/2318%2F103560). PMID 17280321 (https://pubmed.ncbi.nlm.nih.gov/17280321). S2CID 14264923 (https://api.semanticscholar.org/CorpusID:14264923).
38. Aharonovich, I.; et al. (2009). "Enhanced single-photon emission in the near infrared from a diamond color center" (https://rmit-researchmanagement.esploro.exlibrisgroup.com/view/delivery/61RMIT_INST/12246635040001341/13248383310001341). *Physical Review B*. **79** (23): 235316. Bibcode:2009PhRvB..79w5316A (https://ui.adsabs.harvard.edu/abs/2009PhRvB..79w5316A). doi:10.1103/PhysRevB.79.235316 (https://doi.org/10.1103%2FPhysRevB.79.235316). S2CID 37867189 (https://api.semanticscholar.org/CorpusID:37867189).
39. De Weerdt, F.; Collins, A. T.; Zugik, M.; Connor, A. (2005). "Sub-threshold excitation of luminescene of defects in diamonds". *Journal of Physics: Condensed Matter*. **50** (17): 8005. Bibcode:2005JPCM...17.8005D (https://ui.adsabs.harvard.edu/abs/2005JPCM...17.8005D). doi:10.1088/0953-8984/17/50/018 (https://doi.org/10.1088%2F0953-8984%2F17%2F50%2F018). S2CID 97620201 (https://api.semanticscholar.org/CorpusID:97620201).
40. Collins, A. T.; Thomaz, M. F.; Jorge, M. I. B. (1983). "Luminescence decay time of the 1.945 eV centre in type Ib diamond". *Journal of Physics C*. **16** (11): 2177. Bibcode:1983JPhC...16.2177C (https://ui.adsabs.harvard.edu/abs/1983JPhC...16.2177C). doi:10.1088/0022-3719/16/11/020 (https://doi.org/10.1088%2F0022-3719%2F16%2F11%2F020).

41. Hanzawa, H.; Nisida, Y.; Kato, T. (1997). "Measurement of decay time for the NV centre in Ib diamond with a picosecond laser pulse". *Diamond and Related Materials*. **6** (11): 1595. Bibcode:1997DRM.....6.1595H (https://ui.adsabs.harvard.edu/abs/1997DRM.....6.1595H). doi:10.1016/S0925-9635(97)00037-X (https://doi.org/10.1016%2FS0925-9635%2897%2900037-X).
42. Gruber, A.; et al. (1997). "Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers" (http://sites.fas.harvard.edu/~phys191r/References/d4/Gruber1997.pdf) (PDF). *Science*. **276** (5321): 2012–2014. doi:10.1126/science.276.5321.2012 (https://doi.org/10.1126%2Fscience.276.5321.2012).
43. Gordon, Luke; Weber, Justin R.; Varley, Joel B.; Janotti, Anderson; Awschalom, David D.; Van de Walle, Chris G. (2013-10-01). "Quantum computing with defects". *MRS Bulletin*. **38** (10): 802–807. arXiv:1003.1754 (https://arxiv.org/abs/1003.1754). doi:10.1557/mrs.2013.206 (https://doi.org/10.1557%2Fmrs.2013.206).
44. Rogers, L. J.; Doherty, M. W.; Barson, M. S. J.; Onoda, S.; Ohshima, T.; Manson, N. B. (2015-01-01). "Singlet levels of the NV − centre in diamond". *New Journal of Physics*. **17** (1): 013048. arXiv:1407.6244 (https://arxiv.org/abs/1407.6244). Bibcode:2015NJPh...17a3048R (https://ui.adsabs.harvard.edu/abs/2015NJPh...17a3048R). doi:10.1088/1367-2630/17/1/013048 (https://doi.org/10.1088%2F1367-2630%2F17%2F1%2F013048). S2CID 43745993 (https://api.semanticscholar.org/CorpusID:43745993).
45. Rogers, L. J.; Armstrong, S.; Sellars, M. J.; Manson, N. B. (2008). "Infrared emission of the NV centre in diamond: Zeeman and uniaxial stress studies". *New Journal of Physics*. **10** (10): 103024. arXiv:0806.0895 (https://arxiv.org/abs/0806.0895). Bibcode:2008NJPh...10j3024R (https://ui.adsabs.harvard.edu/abs/2008NJPh...10j3024R). doi:10.1088/1367-2630/10/10/103024 (https://doi.org/10.1088%2F1367-2630%2F10%2F10%2F103024). S2CID 42329227 (https://api.semanticscholar.org/CorpusID:42329227).
46. Doherty, Marcus W.; Manson, Neil B.; Delaney, Paul; Jelezko, Fedor; Wrachtrup, Jörg; Hollenberg, Lloyd C.L. (July 2013). "The nitrogen-vacancy colour centre in diamond" (https://linkinghub.elsevier.com/retrieve/pii/S0370157313000562). *Physics Reports*. **528** (1): 1–45. arXiv:1302.3288 (https://arxiv.org/abs/1302.3288). Bibcode:2013PhR...528....1D (https://ui.adsabs.harvard.edu/abs/2013PhR...528....1D). doi:10.1016/j.physrep.2013.02.001 (https://doi.org/10.1016%2Fj.physrep.2013.02.001). S2CID 119113089 (https://api.semanticscholar.org/CorpusID:119113089).
47. Doherty, Marcus W.; Manson, Neil B.; Delaney, Paul; Jelezko, Fedor; Wrachtrup, Jörg; Hollenberg, Lloyd C. L. (2013-07-01). "The nitrogen-vacancy colour centre in diamond". *Physics Reports*. **528** (1): 1–45. arXiv:1302.3288 (https://arxiv.org/abs/1302.3288). Bibcode:2013PhR...528....1D (https://ui.adsabs.harvard.edu/abs/2013PhR...528....1D). CiteSeerX 10.1.1.743.9147 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.743.9147). doi:10.1016/j.physrep.2013.02.001 (https://doi.org/10.1016%2Fj.physrep.2013.02.001). S2CID 119113089 (https://api.semanticscholar.org/CorpusID:119113089).
48. Choi, SangKook (2012-01-01). "Mechanism for optical initialization of spin in NV". *Physical Review B*. **86** (4): 041202. Bibcode:2012PhRvB..86d1202C (https://ui.adsabs.harvard.edu/abs/2012PhRvB..86d1202C). doi:10.1103/PhysRevB.86.041202 (https://doi.org/10.1103%2FPhysRevB.86.041202).
49. Robledo, Lucio; Bernien, Hannes; Sar, Toeno van der; Hanson, Ronald (2011-01-01). "Spin dynamics in the optical cycle of single nitrogen-vacancy centres in diamond". *New Journal of Physics*. **13** (2): 025013. arXiv:1010.1192 (https://arxiv.org/abs/1010.1192). Bibcode:2011NJPh...13b5013R (https://ui.adsabs.harvard.edu/abs/2011NJPh...13b5013R). doi:10.1088/1367-2630/13/2/025013 (https://doi.org/10.1088%2F1367-2630%2F13%2F2%2F025013). S2CID 55207459 (https://api.semanticscholar.org/CorpusID:55207459).

50. Hanson, R.; Gywat, O.; Awschalom, D. D. (2006). "Room-temperature manipulation and decoherence of a single spin in diamond" (https://qutech.nl/wp-content/uploads/2017/03/Room-temperature-manipulation-and-decoherence-of-a-single-spin-in-diamond.pdf) (PDF). *Physical Review B*. **74** (16): 161203. arXiv:quant-ph/0608233 (https://arxiv.org/abs/quant-ph/0608233). Bibcode:2006PhRvB..74p1203H (https://ui.adsabs.harvard.edu/abs/2006PhRvB..74p1203H). doi:10.1103/PhysRevB.74.161203 (https://doi.org/10.1103%2FPhysRevB.74.161203). S2CID 5055366 (https://api.semanticscholar.org/CorpusID:5055366).
51. Dutt, M. V. G.; et al. (2007). "Quantum Register Based on Individual Electronic and Nuclear Spin Qubits in Diamond" (http://www.its.caltech.edu/~ljiang/academic/papers/Quantum_Register_Exp__Science_2007.pdf) (PDF). *Science*. **316** (5829): 1312–6. Bibcode:2007Sci...316.....D (https://ui.adsabs.harvard.edu/abs/2007Sci...316.....D). doi:10.1126/science.1139831 (https://doi.org/10.1126%2Fscience.1139831). PMID 17540898 (https://pubmed.ncbi.nlm.nih.gov/17540898). S2CID 20697722 (https://api.semanticscholar.org/CorpusID:20697722).
52. Childress, L.; et al. (2006). "Coherent Dynamics of Coupled Electron and Nuclear Spin Qubits in Diamond". *Science*. **314** (5797): 281–5. Bibcode:2006Sci...314..281C (https://ui.adsabs.harvard.edu/abs/2006Sci...314..281C). doi:10.1126/science.1131871 (https://doi.org/10.1126%2Fscience.1131871). PMID 16973839 (https://pubmed.ncbi.nlm.nih.gov/16973839). S2CID 18853275 (https://api.semanticscholar.org/CorpusID:18853275).
53. Batalov, A.; et al. (2008). "Temporal Coherence of Photons Emitted by Single Nitrogen-Vacancy Defect Centers in Diamond Using Optical Rabi-Oscillations" (https://www.physik.uni-stuttgart.de/TR21/common/show_file.php/publications/176/publication.pdf) (PDF). *Physical Review Letters*. **100** (7): 077401. Bibcode:2008PhRvL.100g7401B (https://ui.adsabs.harvard.edu/abs/2008PhRvL.100g7401B). doi:10.1103/PhysRevLett.100.077401 (https://doi.org/10.1103%2FPhysRevLett.100.077401). hdl:11858/00-001M-0000-0011-A088-E (https://hdl.handle.net/11858%2F00-001M-0000-0011-A088-E). PMID 18352594 (https://pubmed.ncbi.nlm.nih.gov/18352594).
54. Jelezko, F.; et al. (2004). "Observation of Coherent Oscillations in a Single Electron Spin" (http://capem.buffalo.edu/rashba/PRL76401.pdf) (PDF). *Physical Review Letters*. **92** (7): 076401. Bibcode:2004PhRvL..92g6401J (https://ui.adsabs.harvard.edu/abs/2004PhRvL..92g6401J). doi:10.1103/PhysRevLett.92.076401 (https://doi.org/10.1103%2FPhysRevLett.92.076401). PMID 14995873 (https://pubmed.ncbi.nlm.nih.gov/14995873).
55. Maze, J. R.; Stanwix, P. L.; Hodges, J. S.; Hong, S.; Taylor, J. M.; Cappellaro, P.; Jiang, L.; Dutt, M. V. Gurudev; Togan, E.; Zibrov, A. S.; Yacoby, A. (October 2008). "Nanoscale magnetic sensing with an individual electronic spin in diamond". *Nature*. **455** (7213): 644–647. Bibcode:2008Natur.455..644M (https://ui.adsabs.harvard.edu/abs/2008Natur.455..644M). doi:10.1038/nature07279 (https://doi.org/10.1038%2Fnature07279). PMID 18833275 (https://pubmed.ncbi.nlm.nih.gov/18833275). S2CID 136428582 (https://api.semanticscholar.org/CorpusID:136428582).
56. Degen, C. L.; Reinhard, F.; Cappellaro, P. (2017-07-25). "Quantum sensing". *Reviews of Modern Physics*. **89** (3): 035002. arXiv:1611.02427 (https://arxiv.org/abs/1611.02427). Bibcode:2017RvMP...89c5002D (https://ui.adsabs.harvard.edu/abs/2017RvMP...89c5002D). doi:10.1103/RevModPhys.89.035002 (https://doi.org/10.1103%2FRevModPhys.89.035002). S2CID 2555443 (https://api.semanticscholar.org/CorpusID:2555443).
57. Waldherr, G.; Wang, Y.; Zaiser, S.; Jamali, M.; Schulte-Herbrüggen, T.; Abe, H.; Ohshima, T.; Isoya, J.; Du, J. F.; Neumann, P.; Wrachtrup, J. (February 2014). "Quantum error correction in a solid-state hybrid spin register". *Nature*. **506** (7487): 204–207. arXiv:1309.6424 (https://arxiv.org/abs/1309.6424). Bibcode:2014Natur.506..204W (https://ui.adsabs.harvard.edu/abs/2014Natur.506..204W). doi:10.1038/nature12919 (https://doi.org/10.1038%2Fnature12919). PMID 24476818 (https://pubmed.ncbi.nlm.nih.gov/24476818). S2CID 205237059 (https://api.semanticscholar.org/CorpusID:205237059).

58. MacQuarrie, E. R.; Gosavi, T. A.; Bhave, S. A.; Fuchs, G. D. (2015-12-14). "Continuous dynamical decoupling of a single diamond nitrogen-vacancy center spin with a mechanical resonator". *Physical Review B*. **92** (22): 224419. arXiv:1510.01194 (https://arxiv.org/abs/1510.01194). Bibcode:2015PhRvB..92v4419M (https://ui.adsabs.harvard.edu/abs/2015PhRvB..92v4419M). doi:10.1103/PhysRevB.92.224419 (https://doi.org/10.1103%2FPhysRevB.92.224419). S2CID 53320913 (https://api.semanticscholar.org/CorpusID:53320913).
59. Sasaki, Kento; Monnai, Yasuaki; Saijo, Soya; Fujita, Ryushiro; Watanabe, Hideyuki; Ishi-Hayase, Junko; Itoh, Kohei M.; Abe, Eisuke (2016-05-01). "Broadband, large-area microwave antenna for optically detected magnetic resonance of nitrogen-vacancy centers in diamond". *Review of Scientific Instruments*. **87** (5): 053904. arXiv:1605.04627 (https://arxiv.org/abs/1605.04627). doi:10.1063/1.4952418 (https://doi.org/10.1063%2F1.4952418). PMID 27250439 (https://pubmed.ncbi.nlm.nih.gov/27250439). S2CID 25096136 (https://api.semanticscholar.org/CorpusID:25096136).
60. Teissier, J.; Barfuss, A.; Appel, P.; Neu, E.; Maletinsky, P. (2014-07-10). "Strain Coupling of a Nitrogen-Vacancy Center Spin to a Diamond Mechanical Oscillator" (https://link.aps.org/doi/10.1103/PhysRevLett.113.020503). *Physical Review Letters*. **113** (2): 020503. arXiv:1403.3405 (https://arxiv.org/abs/1403.3405). Bibcode:2014PhRvL.113b0503T (https://ui.adsabs.harvard.edu/abs/2014PhRvL.113b0503T). doi:10.1103/PhysRevLett.113.020503 (https://doi.org/10.1103%2FPhysRevLett.113.020503). PMID 25062153 (https://pubmed.ncbi.nlm.nih.gov/25062153). S2CID 119244679 (https://api.semanticscholar.org/CorpusID:119244679).
61. Grotz, Bernhard; Hauf, Moritz V.; Dankerl, Markus; Naydenov, Boris; Pezzagna, Sébastien; Meijer, Jan; Jelezko, Fedor; Wrachtrup, Jörg; Stutzmann, Martin; Reinhard, Friedemann; Garrido, Jose A. (2012). "Charge state manipulation of qubits in diamond" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3316888). *Nature Communications*. **3** (1): 729. Bibcode:2012NatCo...3..729G (https://ui.adsabs.harvard.edu/abs/2012NatCo...3..729G). doi:10.1038/ncomms1729 (https://doi.org/10.1038%2Fncomms1729). PMC 3316888 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3316888). PMID 22395620 (https://pubmed.ncbi.nlm.nih.gov/22395620).
62. Laraoui, Abdelghani; Aycock-Rizzo, Halley; Gao, Yang; Lu, Xi; Riedo, Elisa; Meriles, Carlos A. (2015). "Imaging thermal conductivity with nanoscale resolution using a scanning spin probe" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4673876). *Nature Communications*. **6** (8954): 8954. arXiv:1511.06916 (https://arxiv.org/abs/1511.06916). Bibcode:2015NatCo...6.8954L (https://ui.adsabs.harvard.edu/abs/2015NatCo...6.8954L). doi:10.1038/ncomms9954 (https://doi.org/10.1038%2Fncomms9954). PMC 4673876 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4673876). PMID 26584676 (https://pubmed.ncbi.nlm.nih.gov/26584676).
63. Maze, J. R.; Stanwix, P. L.; Hodges, J. S.; Hong, S.; Taylor, J. M.; Cappellaro, P.; Jiang, L.; Dutt, M. V. G.; Togan, E.; Zibrov, A. S.; Yacoby, A.; Walsworth, R. L.; Lukin, M. D. (2008). "Nanoscale magnetic sensing with an individual electronic spin in diamond" (https://web.archive.org/web/20160307001934/https://zumbuhllab.unibas.ch/pdf/talks/090821_Sarah_DiamondNV_BSensor.pdf) (PDF). *Nature*. **455** (7213): 644–647. Bibcode:2008Natur.455..644M (https://ui.adsabs.harvard.edu/abs/2008Natur.455..644M). doi:10.1038/nature07279 (https://doi.org/10.1038%2Fnature07279). PMID 18833275 (https://pubmed.ncbi.nlm.nih.gov/18833275). S2CID 136428582 (https://api.semanticscholar.org/CorpusID:136428582). Archived from the original (http://zumbuhllab.unibas.ch/pdf/talks/090821_Sarah_DiamondNV_BSensor.pdf) (PDF) on 2016-03-07. Retrieved 2015-08-29.
64. Dolde, F.; Fedder, H.; Doherty, M. W.; Nöbauer, T.; Rempp, F.; Balasubramanian, G.; Wolf, T.; Reinhard, F.; Hollenberg, L. C. L.; Jelezko, F.; Wrachtrup, J. (2011). "Electric-field sensing using single diamond spins". *Nature Physics*. **7** (6): 459. arXiv:1103.3432 (https://arxiv.org/abs/1103.3432). Bibcode:2011NatPh...7..459D (https://ui.adsabs.harvard.edu/abs/2011NatPh...7..459D). doi:10.1038/nphys1969 (https://doi.org/10.1038%2Fnphys1969). hdl:11858/00-001M-0000-0027-768E-1 (https://hdl.handle.net/11858%2F00-001M-0000-0027-768E-1). S2CID 119287960 (https://api.semanticscholar.org/CorpusID:119287960).

65. Dovzhenko, Y.; Casola, F.; Schlotter, S.; Zhou, T. X.; Büttner, F.; Walsworth, R. L.; Beach, G. S. D.; Yacoby, A. (2018-07-13). "Magnetostatic twists in room-temperature skyrmions explored by nitrogen-vacancy center spin texture reconstruction" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6045603). *Nature Communications*. **9** (1): 2712. Bibcode:2018NatCo...9.2712D (https://ui.adsabs.harvard.edu/abs/2018NatCo...9.2712D). doi:10.1038/s41467-018-05158-9 (https://doi.org/10.1038%2Fs41467-018-05158-9). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 6045603 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6045603). PMID 30006532 (https://pubmed.ncbi.nlm.nih.gov/30006532).
66. Jenkins, Alec; Baumann, Susanne; Zhou, Haoxin; Meynell, Simon A.; Daipeng, Yang; Watanabe, Kenji; Taniguchi, Takashi; Lucas, Andrew; Young, Andrea F.; Bleszynski Jayich, Ania C. (2022-08-17). "Imaging the Breakdown of Ohmic Transport in Graphene" (https://doi.org/10.1103%2FPhysRevLett.129.087701). *Physical Review Letters*. **129** (8): 087701. arXiv:2002.05065 (https://arxiv.org/abs/2002.05065). Bibcode:2022PhRvL.129h7701J (https://ui.adsabs.harvard.edu/abs/2022PhRvL.129h7701J). doi:10.1103/PhysRevLett.129.087701 (https://doi.org/10.1103%2FPhysRevLett.129.087701). PMID 36053708 (https://pubmed.ncbi.nlm.nih.gov/36053708). S2CID 211082922 (https://api.semanticscholar.org/CorpusID:211082922).
67. Scheidegger, P. J.; Diesch, S.; Palm, M. L.; Degen, C. L. (2022-05-30). "Scanning nitrogen-vacancy magnetometry down to 350 mK" (https://doi.org/10.1063/5.0093548). *Applied Physics Letters*. **120** (22). arXiv:2203.15527 (https://arxiv.org/abs/2203.15527). Bibcode:2022ApPhL.120v4001S (https://ui.adsabs.harvard.edu/abs/2022ApPhL.120v4001S). doi:10.1063/5.0093548 (https://doi.org/10.1063%2F5.0093548). ISSN 0003-6951 (https://search.worldcat.org/issn/0003-6951). S2CID 249209788 (https://api.semanticscholar.org/CorpusID:249209788).
68. Stefan, Lucio; Tan, Anthony K.C.; Vindolet, Baptiste; Högen, Michael; Thian, Dickson; Tan, Hang Khume; Rondin, Loïc; Knowles, Helena S.; Roch, Jean-François; Soumyanarayanan, Anjan; Atatüre, Mete (2021-07-22). "Multiangle Reconstruction of Domain Morphology with All-Optical Diamond Magnetometry" (https://link.aps.org/doi/10.1103/PhysRevApplied.16.014054). *Physical Review Applied*. **16** (1): 014054. arXiv:2101.10331 (https://arxiv.org/abs/2101.10331). Bibcode:2021PhRvP..16a4054S (https://ui.adsabs.harvard.edu/abs/2021PhRvP..16a4054S). doi:10.1103/PhysRevApplied.16.014054 (https://doi.org/10.1103%2FPhysRevApplied.16.014054). S2CID 231709827 (https://api.semanticscholar.org/CorpusID:231709827).
69. Zhou, Tony X.; Stöhr, Rainer J.; Yacoby, Amir (2017-10-16). "Scanning diamond NV center probes compatible with conventional AFM technology" (https://doi.org/10.1063/1.4995813). *Applied Physics Letters*. **111** (16). arXiv:1706.09793 (https://arxiv.org/abs/1706.09793). Bibcode:2017ApPhL.111p3106Z (https://ui.adsabs.harvard.edu/abs/2017ApPhL.111p3106Z). doi:10.1063/1.4995813 (https://doi.org/10.1063%2F1.4995813). ISSN 0003-6951 (https://search.worldcat.org/issn/0003-6951). S2CID 4931477 (https://api.semanticscholar.org/CorpusID:4931477).
70. Grazioso, F.; Patton, B. R.; Delaney, P.; Markham, M. L.; Twitchen, D. J.; Smith, J. M. (2013). "Measurement of the full stress tensor in a crystal using photoluminescence from point defects: The example of nitrogen vacancy centers in diamond" (https://pure.qub.ac.uk/portal/en/publications/measurement-of-the-full-stress-tensor-in-a-crystal-using-photoluminescence-from-point-defects-the-example-of-nitrogen-vacancy-centers-in-diamond(2bf91e15-bb44-4c1f-8f8c-ec140c822d80).html). *Applied Physics Letters*. **103** (10): 101905. arXiv:1110.3658 (https://arxiv.org/abs/1110.3658). Bibcode:2013ApPhL.103j1905G (https://ui.adsabs.harvard.edu/abs/2013ApPhL.103j1905G). doi:10.1063/1.4819834 (https://doi.org/10.1063%2F1.4819834). S2CID 119233985 (https://api.semanticscholar.org/CorpusID:119233985).

71. Shao, Linbo; Zhang, Mian; Markham, Matthew; Edmonds, Andrew; Loncar, Marko (15 December 2016). "Diamond Radio Receiver: Nitrogen-Vacancy Centers as Fluorescent Transducers of Microwave Signals" (https://doi.org/10.1103%2FPhysRevApplied.6.064008). *Physical Review Applied*. **6** (6): 064008. Bibcode:2016PhRvP...6f4008S (https://ui.adsabs.harvard.edu/abs/2016PhRvP...6f4008S). doi:10.1103/PhysRevApplied.6.064008 (https://doi.org/10.1103%2FPhysRevApplied.6.064008). S2CID 24851439 (https://api.semanticscholar.org/CorpusID:24851439).
72. Chang, Y.-R.; et al. (2008). "Mass production and dynamic imaging of fluorescent nanodiamonds" (https://web.archive.org/web/20160304052905/http://aao.sinica.edu.tw/download/publication_list/en/149.pdf) (PDF). *Nature Nanotechnology*. **3** (5): 284–8. doi:10.1038/nnano.2008.99 (https://doi.org/10.1038%2Fnnano.2008.99). PMID 18654525 (https://pubmed.ncbi.nlm.nih.gov/18654525). Archived from the original (http://aao.sinica.edu.tw/download/publication_list/en/149.pdf) (PDF) on 2016-03-04. Retrieved 2013-03-04.
73. Nunn, Nicholas; Torelli, Marco D.; Ajoy, Ashok; Smirnov, Alex I.; Shenderova, O. (2022-03-01). "Beauty beyond the Eye: Color Centers in Diamond Particles for Imaging and Quantum Sensing Applications" (https://doi.org/10.1134/S2634827622010044). *Reviews and Advances in Chemistry*. **12** (1): 1–21. doi:10.1134/S2634827622010044 (https://doi.org/10.1134%2FS2634827622010044). ISSN 2634-8284 (https://search.worldcat.org/issn/2634-8284). S2CID 248422954 (https://api.semanticscholar.org/CorpusID:248422954).
74. Chang, Huan-Cheng; Hsiao, Wesley Wei-Wen; Su, Meng-Chih (12 November 2018). *Fluorescent Nanodiamonds* (1 ed.). Wiley. pp. 93–111. ISBN 9781119477082.
75. Chang, Yi-Ren; Lee, Hsu-Yang; Chen, Kowa; Chang, Chun-Chieh; Tsai, Dung-Sheng; Fu, Chi-Cheng; Lim, Tsong-Shin; Tzeng, Yan-Kai; Fang, Chia-Yi; Han, Chau-Chung; Chang, Huan-Cheng; Fann, Wunshain (May 2008). "Mass Production and Dynamic Imaging of Fluorescent Nanodiamonds". *Nature Nanotechnology*. **3** (5): 284–288. doi:10.1038/nnano.2008.99 (https://doi.org/10.1038%2Fnnano.2008.99). PMID 18654525 (https://pubmed.ncbi.nlm.nih.gov/18654525).
76. Aharonovich, I.; Greentree, A. D.; Prawer, S. (2011). "Diamond photonics". *Nature Photonics*. **5** (7): 397. Bibcode:2011NaPho...5..397A (https://ui.adsabs.harvard.edu/abs/2011NaPho...5..397A). doi:10.1038/nphoton.2011.54 (https://doi.org/10.1038%2Fnphoton.2011.54).
77. Jeske, Jan; Lau, Desmond W. M.; Vidal, Xavier; McGuinness, Liam P.; Reineck, Philipp; Johnson, Brett C.; Doherty, Marcus W.; McCallum, Jeffrey C.; Onoda, Shinobu; Jelezko, Fedor; Ohshima, Takeshi; Volz, Thomas; Cole, Jared H.; Gibson, Brant C.; Greentree, Andrew D. (2017). "Stimulated emission from nitrogen-vacancy centres in diamond" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5290152). *Nature Communications*. **8**: 14000. arXiv:1602.07418 (https://arxiv.org/abs/1602.07418). Bibcode:2017NatCo...814000J (https://ui.adsabs.harvard.edu/abs/2017NatCo...814000J). doi:10.1038/ncomms14000 (https://doi.org/10.1038%2Fncomms14000). PMC 5290152 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5290152). PMID 28128228 (https://pubmed.ncbi.nlm.nih.gov/28128228).
78. Breeze, Jonathan D.; Sathian, Juna; Salvadori, Enrico; Alford, Neil McN; Kay, Christopher W. M. (2018-03-21). "Continuous-wave room-temperature diamond maser". *Nature*. **555** (7697): 493–496. arXiv:1710.07726 (https://arxiv.org/abs/1710.07726). Bibcode:2018Natur.555..493B (https://ui.adsabs.harvard.edu/abs/2018Natur.555..493B). doi:10.1038/nature25970 (https://doi.org/10.1038%2Fnature25970). PMID 29565362 (https://pubmed.ncbi.nlm.nih.gov/29565362). S2CID 588265 (https://api.semanticscholar.org/CorpusID:588265).
79. Liu, Ren-Bao (22 March 2018). "A diamond age of masers" (https://doi.org/10.1038%2Fd41586-018-03215-3). *Nature*. **555** (7697): 447–449. Bibcode:2018Natur.555..447L (https://ui.adsabs.harvard.edu/abs/2018Natur.555..447L). doi:10.1038/d41586-018-03215-3 (https://doi.org/10.1038%2Fd41586-018-03215-3). PMID 29565370 (https://pubmed.ncbi.nlm.nih.gov/29565370). S2CID 4143597 (https://api.semanticscholar.org/CorpusID:4143597).

80. Bar-Gill, N.; Pham, L.M.; Jarmola, A.; Budker, D.; Walsworth, R.L. (2012). "Solid-state electronic spin coherence time approaching one second". *Nature Communications*. **4**: 1743. arXiv:1211.7094 (https://arxiv.org/abs/1211.7094). Bibcode:2013NatCo...4.1743B (https://ui.adsabs.harvard.edu/abs/2013NatCo...4.1743B). doi:10.1038/ncomms2771 (https://doi.org/10.1038%2Fncomms2771). PMID 23612284 (https://pubmed.ncbi.nlm.nih.gov/23612284). S2CID 964488 (https://api.semanticscholar.org/CorpusID:964488).
81. Mamin, H. J.; Kim, M.; Sherwood, M. H.; Rettner, C. T.; Ohno, K.; Awschalom, D. D.; Rugar, D. (2013). "Nanoscale Nuclear Magnetic Resonance with a Nitrogen-Vacancy Spin Sensor". *Science*. **339** (6119): 557–560. Bibcode:2013Sci...339..557M (https://ui.adsabs.harvard.edu/abs/2013Sci...339..557M). doi:10.1126/science.1231540 (https://doi.org/10.1126%2Fscience.1231540). PMID 23372008 (https://pubmed.ncbi.nlm.nih.gov/23372008). S2CID 206545959 (https://api.semanticscholar.org/CorpusID:206545959).
82. Hensen, B.; Bernien, H.; Dréau, A.E.; Reiserer, A.; Kalb, N.; Blok, M.S.; Ruitenberg, J.; Vermeulen, R.F.; Schouten, R.N.; Abellán, C.; Amaya, W.; Pruneri, V.; Mitchell, M.W.; Markham, M.; Twitchen, D.J.; Elkouss, D.; Wehner, S.; Taminiau, T.H.; Hanson, R. (2015). "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". *Nature*. **526** (7575): 682–686. arXiv:1508.05949 (https://arxiv.org/abs/1508.05949). Bibcode:2015Natur.526..682H (https://ui.adsabs.harvard.edu/abs/2015Natur.526..682H). doi:10.1038/nature15759 (https://doi.org/10.1038%2Fnature15759). PMID 26503041 (https://pubmed.ncbi.nlm.nih.gov/26503041). S2CID 205246446 (https://api.semanticscholar.org/CorpusID:205246446).
83. Atatüre, Mete; Englund, Dirk; Vamivakas, Nick; Lee, Sang-Yun; Wrachtrup, Joerg (2018). "Material platforms for spin-based photonic quantum technologies". *Nature Reviews Materials*. **3** (5): 38–51. Bibcode:2018NatRM...3...38A (https://ui.adsabs.harvard.edu/abs/2018NatRM...3...38A). doi:10.1038/s41578-018-0008-9 (https://doi.org/10.1038%2Fs41578-018-0008-9). S2CID 139734402 (https://api.semanticscholar.org/CorpusID:139734402).
84. Radko, Ilya P.; Boll, Mads; Israelsen, Niels M.; Raatz, Nicole; Meijer, Jan; Jelezko, Fedor; Andersen, Ulrik L.; Huck, Alexander (2016). "Determining the internal quantum efficiency of shallow-implanted nitrogen-vacancy defects in bulk diamond" (https://backend.orbit.dtu.dk/ws/files/127744471/oe_24_24_27715.pdf) (PDF). *Optics Express*. **24** (24): 27715–27725. Bibcode:2016OExpr..2427715R (https://ui.adsabs.harvard.edu/abs/2016OExpr..2427715R). doi:10.1364/OE.24.027715 (https://doi.org/10.1364%2FOE.24.027715). PMID 27906340 (https://pubmed.ncbi.nlm.nih.gov/27906340).
85. Albrecht, R.; Bommer, A.; Deutsch, C.; Reichel, J.; Becher, C. (2013). "Coupling of a Single Nitrogen-Vacancy Center in Diamond to a Fiber-Based Microcavity". *Physical Review Letters*. **110** (24): 243602. arXiv:1303.7418 (https://arxiv.org/abs/1303.7418). Bibcode:2013PhRvL.110x3602A (https://ui.adsabs.harvard.edu/abs/2013PhRvL.110x3602A). doi:10.1103/physrevlett.110.243602 (https://doi.org/10.1103%2Fphysrevlett.110.243602). PMID 25165921 (https://pubmed.ncbi.nlm.nih.gov/25165921). S2CID 27859868 (https://api.semanticscholar.org/CorpusID:27859868).

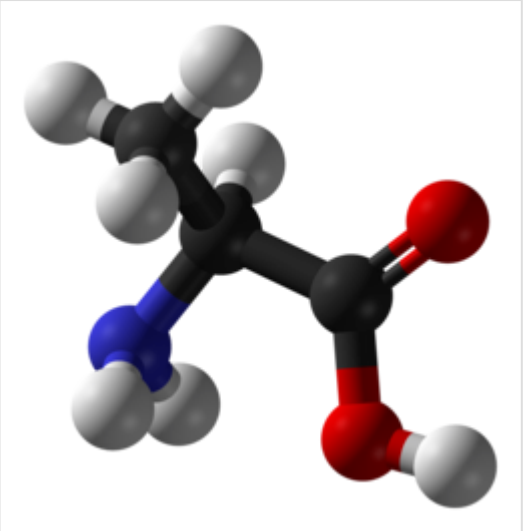
Retrieved from "https://en.wikipedia.org/w/index.php?title=Nitrogen-vacancy_center&oldid=1232507042"

WIKIPEDIA
The Free Encyclopedia

Nuclear magnetic resonance quantum computer

Nuclear magnetic resonance quantum computing (**NMRQC**)[1] is one of the several proposed approaches for constructing a quantum computer, that uses the spin states of nuclei within molecules as qubits. The quantum states are probed through the nuclear magnetic resonances, allowing the system to be implemented as a variation of nuclear magnetic resonance spectroscopy. NMR differs from other implementations of quantum computers in that it uses an ensemble of systems, in this case molecules, rather than a single pure state.

Initially the approach was to use the spin properties of atoms of particular molecules in a liquid sample as qubits - this is known as liquid state NMR (LSNMR). This approach has since been superseded by solid state NMR (SSNMR) as a means of quantum computation.



Molecule of alanine used in NMR implementation of quantum computing. Qubits are implemented by spin states of the black carbon atoms

Liquid state NMR

The ideal picture of liquid state NMR (LSNMR) quantum information processing (QIP) is based on a molecule in which some of its atom's nuclei behave as spin-$\frac{1}{2}$ systems.[2] Depending on which nuclei we are considering they will have different energy levels and different interaction with its neighbours and so we can treat them as distinguishable qubits. In this system we tend to consider the inter-atomic bonds as the source of interactions between qubits and exploit these spin-spin interactions to perform 2-qubit gates such as CNOTs that are necessary for universal quantum computation. In addition to the spin-spin interactions native to the molecule an external magnetic field can be applied (in NMR laboratories) and these impose single qubit gates. By exploiting the fact that different spins will experience different local fields we have control over the individual spins.

The picture described above is far from realistic since we are treating a single molecule. NMR is performed on an ensemble of molecules, usually with as many as 10^15 molecules. This introduces complications to the model, one of which is introduction of decoherence. In particular we have the problem of an open quantum system interacting with a macroscopic number of particles near thermal equilibrium (~mK to ~300 K). This has led the development of decoherence suppression techniques that have spread to other disciplines such as trapped ions. The other significant issue with regards to working

close to thermal equilibrium is the mixedness of the state. This required the introduction of ensemble quantum processing, whose principal limitation is that as we introduce more logical qubits into our system we require larger samples in order to attain discernable signals during measurement.

Solid state NMR

Solid state NMR (SSNMR), unlike LSNMR uses a solid state sample, for example a nitrogen vacancy diamond lattice rather than a liquid sample.[3] This has many advantages such as lack of molecular diffusion decoherence, lower temperatures can be achieved to the point of suppressing phonon decoherence and a greater variety of control operations that allow us to overcome one of the major problems of LSNMR that is initialisation. Moreover, as in a crystal structure we can localize precisely the qubits, we can measure each qubit individually, instead of having an ensemble measurement as in LSNMR.

History

The use of nuclear spins for quantum computing was first discussed by Seth Lloyd and by David DiVincenzo.[4][5][6] Manipulation of nuclear spins for quantum computing using liquid state NMR was introduced independently by Cory, Fahmy and Havel[7][8] and Gershenfeld and Chuang[9] in 1997. Some early success was obtained in performing quantum algorithms in NMR systems due to the relative maturity of NMR technology. For instance, in 2001 researchers at IBM reported the successful implementation of Shor's algorithm in a 7-qubit NMR quantum computer.[10] However, even from the early days, it was recognized that NMR quantum computers would never be very useful due to the poor scaling of the signal-to-noise ratio in such systems.[11] More recent work, particularly by Caves and others, shows that all experiments in liquid state bulk ensemble NMR quantum computing to date do not possess quantum entanglement, thought to be required for quantum computation. Hence NMR quantum computing experiments are likely to have been only classical simulations of a quantum computer.[12]

Mathematical representation

The ensemble is initialized to be the thermal equilibrium state (see quantum statistical mechanics). In mathematical parlance, this state is given by the density matrix:

$$\rho = \frac{e^{-\beta H}}{\mathrm{Tr}(e^{-\beta H})},$$

where H is the hamiltonian matrix of an individual molecule and

$$\beta = \frac{1}{kT}$$

where k is the Boltzmann constant and T the temperature. That the initial state in NMR quantum computing is in thermal equilibrium is one of the main differences compared to other quantum computing techniques, where they are initialized in a pure state. Nevertheless, suitable mixed states are capable of

reflecting quantum dynamics which lead to Gershenfeld and Chuang to term them "pseudo-pure states".[9]

Operations are performed on the ensemble through radio frequency (RF) pulses applied perpendicular to a strong, static magnetic field, created by a very large magnet. See nuclear magnetic resonance.

Consider applying a magnetic field along the z axis, fixing this as the principal quantization axis, on a liquid sample. The Hamiltonian for a single spin would be given by the Zeeman or chemical shift term:

$$H = \mu B_z = I_z \omega$$

where I_z is the operator for the z component of the nuclear angular momentum, and ω is the resonance frequency of the spin, which is proportional to the applied magnetic field.

Considering the molecules in the liquid sample to contain two spin-$\frac{1}{2}$ nuclei, the system Hamiltonian will have two chemical shift terms and a dipole coupling term:

$$H = \omega_1 I_{z1} + \omega_2 I_{z2} + 2J_{12} I_{z1} I_{z2}$$

Control of a spin system can be realized by means of selective RF pulses applied perpendicular to the quantization axis. In the case of a two spin system as described above, we can distinguish two types of pulses: "soft" or spin-selective pulses, whose frequency range encompasses one of the resonant frequencies only, and therefore affects only that spin; and "hard" or nonselective pulses whose frequency range is broad enough to contain both resonant frequencies and therefore these pulses couple to both spins. For detailed examples of the effects of pulses on such a spin system, the reader is referred to Section 2 of work by Cory et al.[13]

See also

- Kane quantum computer

References

1. "Nuclear Magnetic Resonance Quantum Computing (NMRQC)" (http://web.physics.ucsb.edu/~msteffen/nmrqc.htm).
2. Neil Gershenfeld; Isaac L. Chuang (1998). "Quantum computing with molecules" (http://cba.mit.edu/docs/papers/98.06.sciqc.pdf) (PDF). *Scientific American*. **278** (6): 66–71. Bibcode:1998SciAm.278f..66G (https://ui.adsabs.harvard.edu/abs/1998SciAm.278f..66G). doi:10.1038/scientificamerican0698-66 (https://doi.org/10.1038%2Fscientificamerican0698-66).
3. "Diamond Sparkles in Quantum Computing" (https://www.aps.org/publications/apsnews/200805/diamond.cfm).
4. Seth Lloyd (1993). "A Potentially Realizable Quantum Computer". *Science*. **261** (5128): 1569–1571. Bibcode:1993Sci...261.1569L (https://ui.adsabs.harvard.edu/abs/1993Sci...261.1569L). doi:10.1126/science.261.5128.1569 (https://doi.org/10.1126%2Fscience.261.5128.1569). PMID 17798117 (https://pubmed.ncbi.nlm.nih.gov/17798117). S2CID 38100483 (https://api.semanticscholar.org/CorpusID:38100483).

5. David DiVincenzo (1995). "A Two-bit gates are universal for quantum computation". *Phys. Rev. A*. **51** (2): 1015–1022. arXiv:cond-mat/9407022 (https://arxiv.org/abs/cond-mat/9407022). Bibcode:1995PhRvA..51.1015D (https://ui.adsabs.harvard.edu/abs/1995PhRvA..51.1015D). doi:10.1103/PhysRevA.51.1015 (https://doi.org/10.1103%2FPhysRevA.51.1015). PMID 9911679 (https://pubmed.ncbi.nlm.nih.gov/9911679). S2CID 2317415 (https://api.semanticscholar.org/CorpusID:2317415).
6. David DiVincenzo (1995). "Quantum computation". *Science*. **270** (5234).
7. Cory, David G.; Fahmy, Amr F.; Havel, Timothy F. (1996). "Nuclear Magnetic Resonance Spectroscopy: An Experimentally Accessible Paradigm for Quantum Computing". Phys-Comp 96, Proceedings of the Fourth Workshop on Physics and Computation, edited by T.Toffoli, M.Biafore, and J.Leao (New England Complex Systems Institute. pp. 87–91.
8. Cory, David G.; Fahmy, Amr F.; Havel, Timothy F. (1997-03-04). "Ensemble quantum computing by NMR spectroscopy" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC19968). *Proceedings of the National Academy of Sciences*. **94** (5): 1634–1639. Bibcode:1997PNAS...94.1634C (https://ui.adsabs.harvard.edu/abs/1997PNAS...94.1634C). doi:10.1073/pnas.94.5.1634 (https://doi.org/10.1073%2Fpnas.94.5.1634). ISSN 0027-8424 (https://search.worldcat.org/issn/0027-8424). PMC 19968 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC19968). PMID 9050830 (https://pubmed.ncbi.nlm.nih.gov/9050830).
9. Gershenfeld, Neil A.; Chuang, Isaac L. (1997-01-17). "Bulk Spin-Resonance Quantum Computation". *Science*. **275** (5298): 350–356. CiteSeerX 10.1.1.28.8877 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.28.8877). doi:10.1126/science.275.5298.350 (https://doi.org/10.1126%2Fscience.275.5298.350). ISSN 0036-8075 (https://search.worldcat.org/issn/0036-8075). PMID 8994025 (https://pubmed.ncbi.nlm.nih.gov/8994025). S2CID 2262147 (https://api.semanticscholar.org/CorpusID:2262147).
10. Vandersypen LM, Steffen M, Breyta G, Yannoni CS, Sherwood MH, Chuang IL (2001). "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". *Nature*. **414** (6866): 883–887. arXiv:quant-ph/0112176 (https://arxiv.org/abs/quant-ph/0112176). Bibcode:2001Natur.414..883V (https://ui.adsabs.harvard.edu/abs/2001Natur.414..883V). doi:10.1038/414883a (https://doi.org/10.1038%2F414883a). PMID 11780055 (https://pubmed.ncbi.nlm.nih.gov/11780055). S2CID 4400832 (https://api.semanticscholar.org/CorpusID:4400832).
11. Warren WS (1997). "The usefulness of NMR quantum computing". *Science*. **277** (5332): 1688–1689. doi:10.1126/science.277.5332.1688 (https://doi.org/10.1126%2Fscience.277.5332.1688).
12. Menicucci NC, Caves CM (2002). "Local realistic model for the dynamics of bulk-ensemble NMR information processing". *Physical Review Letters*. **88** (16): 167901. arXiv:quant-ph/0111152 (https://arxiv.org/abs/quant-ph/0111152). Bibcode:2002PhRvL..88p7901M (https://ui.adsabs.harvard.edu/abs/2002PhRvL..88p7901M). doi:10.1103/PhysRevLett.88.167901 (https://doi.org/10.1103%2FPhysRevLett.88.167901). PMID 11955265 (https://pubmed.ncbi.nlm.nih.gov/11955265). S2CID 14583916 (https://api.semanticscholar.org/CorpusID:14583916).
13. Cory D.; et al. (1998). "Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing". *Physica D*. **120** (1–2): 82–101. arXiv:quant-ph/9709001 (https://arxiv.org/abs/quant-ph/9709001). Bibcode:1998PhyD..120...82C (https://ui.adsabs.harvard.edu/abs/1998PhyD..120...82C). doi:10.1016/S0167-2789(98)00046-3 (https://doi.org/10.1016%2FS0167-2789%2898%2900046-3). S2CID 219400 (https://api.semanticscholar.org/CorpusID:219400).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Nuclear_magnetic_resonance_quantum_computer&oldid=1230036470"

WIKIPEDIA
The Free Encyclopedia

Superconducting quantum computing

Superconducting quantum computing is a branch of solid state quantum computing that implements superconducting electronic circuits using superconducting qubits as artificial atoms, or quantum dots. For superconducting qubits, the two logic states are the ground state and the excited state, denoted $|g\rangle$ **and** $|e\rangle$respectively.[1] Research in superconducting quantum computing is conducted by companies such as Google,[2] IBM,[3] IMEC,[4] BBN Technologies,[5] Rigetti,[6] and Intel.[7] Many recently developed QPUs (quantum processing units, or quantum chips) use superconducting architecture.

As of May 2016, up to 9 fully controllable qubits are demonstrated in the 1D array,[8] and up to 16 in 2D architecture.[3] In October 2019, the Martinis group, partnered with Google, published an article demonstrating novel quantum supremacy, using a chip composed of 53 superconducting qubits.[9]

Background

Classical computation models rely on physical implementations consistent with the laws of classical mechanics.[10] Classical descriptions are accurate only for specific systems consisting of a relatively large number of atoms. A more general description of nature is given by quantum mechanics. Quantum computation studies quantum phenomena applications beyond the scope of classical approximation, with the purpose of performing quantum information processing and communication. Various models of quantum computation exist, but the most popular models incorporate concepts of qubits and quantum gates (or gate-based superconducting quantum computing).

Superconductors are implemented due to the fact that at low temperatures they have infinite conductivity and zero resistance. Each qubit is built using semiconductor circuits with an LC circuit: a capacitor and an inductor.

Superconducting capacitors and inductors are used to produce a resonant circuit that dissipates almost no energy, as heat can disrupt quantum information. The superconducting resonant circuits are a class of artificial atoms that can be used as qubits. Theoretical and physical implementations of quantum circuits are widely different. Implementing a quantum circuit had its own set of challenges and must abide by DiVincenzo's criteria, conditions proposed by theoretical physicist David P DiVincenzo,[11] which is set of criteria for the physical implementation of superconducting quantum computing, where the initial five criteria ensure that the quantum computer is in line with the postulates of quantum mechanics and the remaining two pertaining to the relaying of this information over a network.

We map the ground and excited states of these atoms to the 0 and 1 state as these are discrete and distinct energy values and therefore it is in line with the postulates of quantum mechanics. In such a construction however an electron can jump to multiple other energy states and not be confined to our excited state; therefore, it is imperative that the system be limited to be affected only by photons with energy difference required to jump from the ground state to the excited state.[12] However, this leaves one major issue, we require uneven spacing between our energy levels to prevent photons with the same energy from causing transitions between neighboring pairs of states. Josephson junctions are superconducting elements with a nonlinear inductance, which is critically important for qubit implementation.[12] The use of this nonlinear element in the resonant superconducting circuit produces uneven spacings between the energy levels.

Qubits

A qubit is a generalization of a bit (a system with two possible states) capable of occupying a quantum superposition of both states. A quantum gate, on the other hand, is a generalization of a logic gate describing the transformation of one or more qubits once a gate is applied given their initial state. Physical implementation of qubits and gates is challenging for the same reason that quantum phenomena are difficult to observe in everyday life given the minute scale on which they occur. One approach to achieving quantum computers is by implementing superconductors whereby quantum effects are macroscopically observable, though at the price of extremely low operation temperatures.

Superconductors

Unlike typical conductors, superconductors possess a critical temperature at which resistivity plummets to nearly zero and conductivity is drastically increased. In superconductors, the basic charge carriers are pairs of electrons (known as Cooper pairs), rather than single fermions as found in typical conductors.[13] Cooper pairs are loosely bound and have an energy state lower than that of Fermi Energy. Electrons forming Cooper pairs possess equal and opposite momentum and spin so that the total spin of the Cooper pair is an integer spin. Hence, Cooper pairs are bosons. Two such superconductors which have been used in superconducting qubit models are niobium and tantalum, both d-band superconductors.[14]

Bose-Einstein condensates

Once cooled to nearly absolute zero, a collection of bosons collapse into their lowest energy quantum state (the ground state) to form a state of matter known as Bose–Einstein condensate. Unlike fermions, bosons may occupy the same quantum energy level (or quantum state) and do not obey the Pauli exclusion principle. Classically, Bose-Einstein Condensate can be conceptualized as multiple particles occupying the same position in space and having equal momentum. Because interactive forces between bosons are minimized, Bose-Einstein Condensates effectively act as a superconductor. Thus, superconductors are implemented in quantum computing because they possess both near infinite conductivity and near zero resistance. The advantages of a superconductor over a typical conductor, then, are twofold in that superconductors can, in theory, transmit signals nearly

instantaneously and run infinitely with no energy loss. The prospect of actualizing superconducting quantum computers becomes all the more promising considering NASA's recent development of the Cold Atom Lab in outer space where Bose-Einstein Condensates are more readily achieved and sustained (without rapid dissipation) for longer periods of time without the constraints of gravity.[15]

Electrical circuits

At each point of a superconducting electronic circuit (a network of electrical elements), the condensate wave function describing charge flow is well-defined by some complex probability amplitude. In typical conductor electrical circuits, this same description is true for individual charge carriers except that the various wave functions are averaged in macroscopic analysis, making it impossible to observe quantum effects. The condensate wave function becomes useful in allowing design and measurement of macroscopic quantum effects. Similar to the discrete atomic energy levels in the Bohr model, only discrete numbers of magnetic flux quanta can penetrate a superconducting loop. In both cases, quantization results from complex amplitude continuity. Differing from microscopic implementations of quantum computers (such as atoms or photons), parameters of superconducting circuits are designed by setting (classical) values to the electrical elements composing them such as by adjusting capacitance or inductance.

To obtain a quantum mechanical description of an electrical circuit, a few steps are required. Firstly, all electrical elements must be described by the condensate wave function amplitude and phase rather than by closely related macroscopic current and voltage descriptions used for classical circuits. For instance, the square of the wave function amplitude at any arbitrary point in space corresponds to the probability of finding a charge carrier there. Therefore, the squared amplitude corresponds to a classical charge distribution. The second requirement to obtain a quantum mechanical description of an electrical circuit is that generalized Kirchhoff's circuit laws are applied at every node of the circuit network to obtain the system's equations of motion. Finally, these equations of motion must be reformulated to Lagrangian mechanics such that a quantum Hamiltonian is derived describing the total energy of the system.

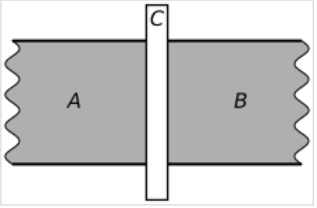
Technology

Manufacturing

Superconducting quantum computing devices are typically designed in the radio-frequency spectrum, cooled in dilution refrigerators below 15 mK and addressed with conventional electronic instruments, e.g. frequency synthesizers and spectrum analyzers. Typical dimensions fall on the range of micrometers, with sub-micrometer resolution, allowing for the convenient design of a Hamiltonian system with well-established integrated circuit technology. Manufacturing superconducting qubits follows a process involving lithography, depositing of metal, etching, and controlled oxidation as described in.[16] Manufacturers continue to improve the lifetime of superconducting qubits and have made significant improvements since the early 2000s.[16]:4

Josephson junctions

One distinguishable attribute of superconducting quantum circuits is the use of Josephson junctions. Josephson junctions are an electrical element which does not exist in normal conductors. Recall that a junction is a weak connection between two leads of wire (in this case a superconductive wire) on either side of a thin layer of insulator material only a few atoms thick, usually implemented using shadow evaporation technique. The resulting Josephson junction device exhibits the Josephson Effect whereby the junction produces a supercurrent. An image of a single Josephson junction is shown to the right. The condensate wave function on the two sides of the junction are weakly correlated, meaning that they are allowed to have different superconducting phases. This distinction of nonlinearity contrasts continuous superconducting wire for which the wave function across the junction must be continuous. Current flow through the junction occurs by quantum tunneling, seeming to instantaneously "tunnel" from one side of the junction to the other. This tunneling phenomenon is unique to quantum systems. Thus, quantum tunneling is used to create nonlinear inductance, essential for qubit design as it allows a design of anharmonic oscillators for which energy levels are discretized (or quantized) with nonuniform spacing between energy levels, denoted ΔE.[1] In contrast, the quantum harmonic oscillator *cannot* be used as a qubit as there is no way to address only two of its states, given that the spacing between every energy level and the next is exactly the same.



A single Josephson junction where C is a thin layer of insulator and A & B are (superconducting) currents with nonequivalent wave functions

Qubit archetypes

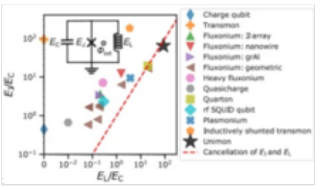
The three primary superconducting qubit archetypes are the phase, charge and flux qubit. Many hybridizations of these archetypes exist including the fluxonium,[17] transmon,[18] Xmon,[19] and quantronium.[20] For any qubit implementation the logical quantum states $\{|0\rangle, |1\rangle\}$ are mapped to different states of the physical system (typically to discrete energy levels or their quantum superpositions). Each of the three archetypes possess a distinct range of Josephson energy to charging energy ratio. Josephson energy refers to the energy stored in Josephson junctions when current passes through, and charging energy is the energy required for one Cooper pair to charge the junction's total capacitance.[21] Josephson energy can be written as

$$U_j = -\frac{I_0 \Phi_0}{2\pi} \cos\delta,$$

where I_0 is the critical current parameter of the Josephson junction, $\Phi_0 = \frac{h}{2e}$ is (superconducting) flux quantum, and δ is the phase difference across the junction.[21] Notice that the term $cos\delta$ indicates nonlinearity of the Josephson junction.[21] Charge energy is written as

$$E_C = \frac{e^2}{2C},$$

where C is the junction's capacitance and e is electron charge.[21] Of the three archetypes, phase qubits allow the most of Cooper pairs to tunnel through the junction, followed by flux qubits, and charge qubits allow the fewest.



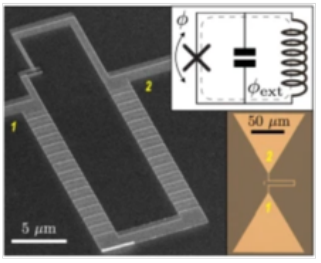
A graph of various superconducting qubit archetypes by their Josephson energy to charging energy ratio with a legend on the right.[22] The top left graphic illustrates a unimon electrical circuit.[22]

Phase qubit

The phase qubit possesses a Josephson to charge energy ratio on the order of magnitude 10^6. For phase qubits, energy levels correspond to different quantum charge oscillation amplitudes across a Josephson junction, where charge and phase are analogous to momentum and position respectively as analogous to a quantum harmonic oscillator. Note that in this context phase is the complex argument of the superconducting wave function (also known as the superconducting order parameter), not the phase between the different states of the qubit.

Flux qubit

The flux qubit (also known as a persistent-current qubit) possesses a Josephson to charging energy ratio on the order of magnitude 10. For flux qubits, the energy levels correspond to different integer numbers of magnetic flux quanta trapped in a superconducting ring.



The left-most image shows a fluxonium superconducting loop consisting of a collection of larger area Josephson junctions and one smaller area Josephson junction, as shown by an electron microscope.[23] The top right image depicts fluxonium circuit components, and the bottom right image depicts a smaller area Josephson junction.[23]

Fluxonium

Fluxonium qubits are a specific type of flux qubit whose Josephson junction is shunted by a linear inductor of $E_J \gg E_L$ where $E_L = (\hbar/2e)^2/L$.[24] In practice, the linear inductor is usually implemented by a Josephson junction array that is composed of a large number (can be often $N > 100$) of large-sized Josephson junctions connected in a series. Under this condition, the Hamiltonian of a fluxonium can be written as:

$$\hat{H} = 4E_C\hat{n}^2 + \frac{1}{2}E_L(\hat{\phi} - \phi_{ext})^2 - E_J\cos\hat{\phi}.$$

One important property of the fluxonium qubit is the longer qubit lifetime at the half flux sweet spot, which can exceed 1 millisecond.[24][25] Another crucial advantage of the fluxonium qubit biased at the sweet spot is the large anharmonicity, which allows fast local microwave control and mitigates spectral crowding problems, leading to better scalability.[26][27]

Charge qubit

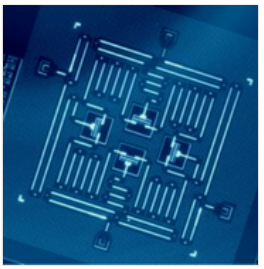
The charge qubit, also known as the Cooper pair box, possesses a Josephson to charging energy ratio on the order of magnitude < 1. For charge qubits, different energy levels correspond to an integer number of Cooper pairs on a superconducting island (a small superconducting area with a controllable number of charge carriers).[28] Indeed, the first experimentally realized qubit was the Cooper pair box, achieved in 1999.[29]

Transmon

Transmons are a special type of qubit with a shunted capacitor specifically designed to mitigate noise. The transmon qubit model was based on the Cooper pair box[31] (illustrated in the table above in row one column one). It was also the first qubit to demonstrate quantum supremacy.[32] The increased ratio of Josephson to charge energy mitigates noise. Two transmons can be coupled using a coupling capacitor.[1] For this 2-qubit system the Hamiltonian is written

$$\hat{H} = \frac{\hbar J}{2}(\sigma_1^x\sigma_2^x + \sigma_1^y\sigma_2^y),$$

where J is current density and σ is surface charge density.[1]



A device consisting of four superconducting transmon qubits, four quantum buses, and four readout resonators fabricated by IBM and published in npj Quantum Information in January 2017[30]

Xmon

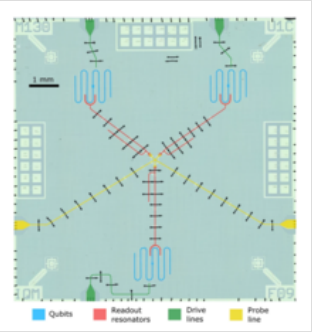
The Xmon is very similar in design to a transmon in that it originated based on the planar transmon model.[33] An Xmon is essentially a tunable transmon. The major distinguishing difference between transmon and Xmon qubits is the Xmon qubits is grounded with one of its capacitor pads.[34]

Gatemon

Another variation of the transmon qubit is the Gatemon. Like the Xmon, the Gatemon is a tunable variation of the transmon. The Gatemon is tunable via gate voltage.

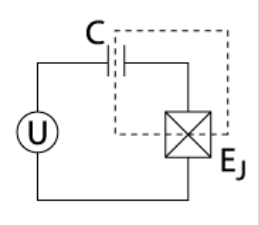
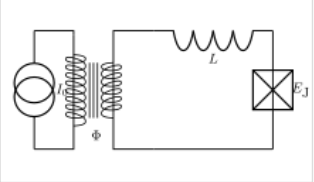
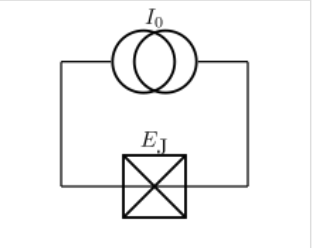
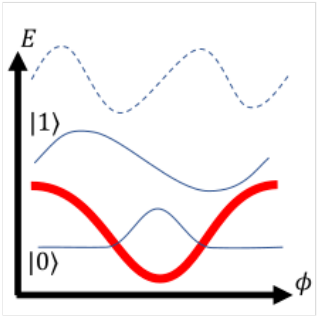
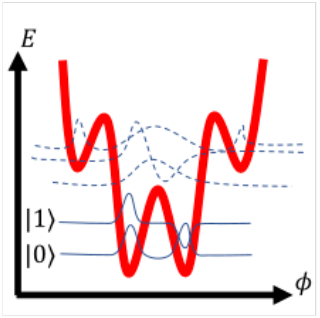
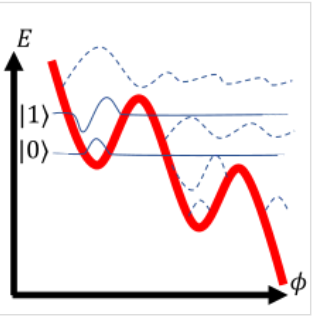
Unimon

In 2022 researchers from IQM Quantum Computers, Aalto University, and VTT Technical Research Centre of Finland discovered a novel superconducting qubit known as the Unimon.[36] A relatively simple qubit, the Unimon consists of a single Josephson junction shunted by a linear inductor (possessing an inductance not depending on current) inside a (superconducting) resonator.[37] Unimons have increased anharmocity and display faster operation time resulting in lower susceptibility to noise errors.[37] In addition to increased anharmocity, other advantages Unimon qubit include decreased susceptibility to flux noise and complete insensitivity to dc charge noise.[22]



Superconducting circuit consisting of 3 Unimons (blue), each connected to resonators (red), drive lines (green), and joint probe lines (yellow)[35]

Superconducting Qubit Archetypes [38]

Type / Aspect	Charge qubit	RF-SQUID qubit (prototype of the Flux Qubit)	Phase qubit
Circuit	 Charge qubit circuit. A superconducting island (encircled with a dashed line) is defined between the leads of a capacitor with capacitance C and a Josephson junction with energy E_J biased by voltage U.	 Flux qubit circuit. A superconducting loop with inductance L is interrupted by a junction with Josephson energy E_J. Bias flux Φ is induced by a flux line with current I_0.	 Phase qubit circuit. A Josephson junction with energy parameter E_J is biased by current I_0.
Hamiltonian	$H = E_C(N - N_g)^2 - E_J \cos\phi$ In this case N is the number of Cooper pairs to tunnel through the junction, $N_g = CV_0/2e$ is the charge on the capacitor in units of Cooper pairs number, $E_C = (2e)^2/2(C_J + C)$ is the charging energy associated with both capacitance C and Josephson junction capacitance C_J.	$H = \frac{q^2}{2C_J} + \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{\phi^2}{2L} - E_J \cos\left[\phi - \Phi\frac{2\pi}{\Phi_0}\right]$ Note that ϕ is only allowed to take values greater than 2π and is alternatively defined as the time integral of voltage along inductance L.	$H = \frac{(2e)^2}{2C_J}q^2 - I_0\frac{\Phi_0}{2\pi}\phi - E_J\cos\phi$ Here Φ_0 is magnetic flux quantum.
Potential	 $U = -E_J\cos\phi$. Bias voltage is set such that $N_g = \frac{1}{2}$, minimizing the energy gap between $\|0\rangle$ and $\|1\rangle$, consequently distinguishing the gap from other energy gaps (e.g. gap between $\|1\rangle$ and $\|2\rangle$). The difference in gaps allows addressing transitions from $\|0\rangle$ to $\|1\rangle$ and vice versa only, without populating other states.	 $U = \left(\frac{\Phi_0}{2\pi}\right)^2 \frac{\phi^2}{2L} - E_J\cos\left[\phi - \Phi\frac{2\pi}{\Phi_0}\right]$ Bias flux is $\Phi = \Phi_0/2$. Different wells correspond to a distinct number of flux quanta trapped in the superconducting loops. The two lower states correspond to a symmetrical and anti-symmetrical superposition of zero or single trapped flux quanta, sometimes denoted as clockwise and counterclockwise loop current states: $\|0\rangle = [|\circlearrowleft\rangle + |\circlearrowright\rangle]/\sqrt{2}$ and $\|1\rangle = [|\circlearrowleft\rangle - |\circlearrowright\rangle]/\sqrt{2}$.	 $U = -I_0\frac{\Phi_0}{2\pi}\phi - E_J\cos\phi$, also known as "washboard" potential. Bias current is adjusted to allow wells shallow enough to contain exactly two localized wave functions. A slight increase in bias current causes a selective "spill" of higher energy state ($\|1\rangle$), expressed with a measurable voltage spike (a mechanism commonly used for phase qubit measurement).

In the table above, the three superconducting qubit archetypes are reviewed. In the first row, the qubit's electrical circuit diagram is presented. The second row depicts a quantum Hamiltonian derived from the circuit. Generally, the Hamiltonian is the sum of the system's kinetic and potential energy components (analogous to a particle in a potential well). For the Hamiltonians denoted, ϕ is the superconducting wave function phase difference across the junction, C_J is the capacitance associated with the Josephson junction, and q is the charge on the junction capacitance. For each potential depicted, only solid wave functions are used for computation. The qubit potential is indicated by a thick red line, and schematic wave function solutions are depicted by thin lines, lifted to their appropriate energy level for clarity.

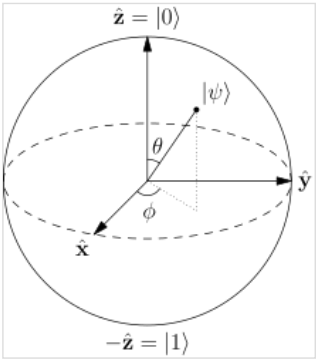
Note that particle mass corresponds to an inverse function of the circuit capacitance and that the shape of the potential is governed by regular inductors and Josephson junctions. Schematic wave solutions in the third row of the table show the complex amplitude of the phase variable. Specifically, if a qubit's phase is measured while the qubit occupies a particular state, there is a non-zero probability of measuring a specific value *only* where the depicted wave function oscillates. All three rows are essentially different presentations of the same physical system.

Single qubits

The GHz energy gap between energy levels of a superconducting qubit is designed to be compatible with available electronic equipment, due to the terahertz gap (lack of equipment in the higher frequency band). The superconductor energy gap implies a top limit of operation below ~1THz beyond which Cooper pairs break, so energy level separation cannot be too high. On the other hand, energy level separation cannot be too small due to cooling considerations: a temperature of 1 K implies energy fluctuations of 20 GHz. Temperatures of tens of millikelvins are achieved in dilution refrigerators and allow qubit operation at a ~5 GHz energy level separation. Qubit energy level separation is frequently adjusted by controlling a dedicated bias current line, providing a "knob" to fine tune the qubit parameters.

Single qubit gates

A single qubit gate is achieved by rotation in the Bloch sphere. Rotations between different energy levels of a single qubit are induced by microwave pulses sent to an antenna or transmission line coupled to the qubit with a frequency resonant with the energy separation between levels. Individual qubits may be addressed by a dedicated transmission line or by a shared one if the other qubits are off resonance. The axis of rotation is set by quadrature amplitude modulation of microwave pulse, while pulse length determines the angle of rotation.[39]



A depiction of the Bloch sphere

More formally (following the notation of [39]) for a driving signal

$$\mathcal{E}(t) = \mathcal{E}^x(t)\cos(\omega_d t) + \mathcal{E}^y(t)\sin(\omega_d t)$$

of frequency ω_d, a driven qubit Hamiltonian in a rotating wave approximation is

$$H^R/\hbar = (\omega - \omega_d)|1\rangle\langle 1| + \frac{\mathcal{E}^x(t)}{2}\sigma_x + \frac{\mathcal{E}^y(t)}{2}\sigma_y,$$

where ω is the qubit resonance and σ_x, σ_y are Pauli matrices.

To implement a rotation about the X axis, one can set $\mathcal{E}^y(t) = 0$ and apply a microwave pulse at frequency $\omega_d = \omega$ for time t_g. The resulting transformation is

$$U_x = \exp\left\{-\frac{i}{\hbar}\int_0^{t_g} H^R dt\right\} = \exp\left\{-i\int_0^{t_g} \mathcal{E}^x(t)dt \cdot \sigma_x/2\right\}.$$

This is exactly the rotation operator $R_X(\theta)$ by angle $\theta = \int_0^{t_g} \mathcal{E}^x(t)dt$ about the X axis in the Bloch sphere. A rotation about the Y axis can be implemented in a similar way. Showing the two rotation operators is sufficient for satisfying universality as every single qubit unitary operator U may be presented as $U = R_X(\theta_1)R_Y(\theta_2)R_X(\theta_3)$ (up to a global phase which is physically inconsequential) by a procedure known as the $X-Y$ decomposition.[40] Setting $\int_0^{t_g} \mathcal{E}^x(t)dt = \pi$ results in the transformation

$$U_x = \exp\left\{-i\int_0^{t_g} \mathcal{E}^x(t)dt \cdot \sigma_x/2\right\} = e^{-i\pi\sigma_x/2} = -i\sigma_x$$

up to the global phase $-i$ and is known as the NOT gate.

Coupling qubits

The ability to couple qubits is essential for implementing 2-qubit gates. Coupling two qubits can be achieved by connecting both to an intermediate electrical coupling circuit. The circuit may be either a fixed element (such as a capacitor) or be controllable (like the DC-SQUID). In the first case, decoupling qubits during the time the gate is switched off is achieved by tuning qubits out of resonance one from another, making the energy gaps between their computational states different.[41] This approach is inherently limited to nearest-neighbor coupling since a physical electrical circuit must be laid out between connected qubits. Notably, D-Wave Systems' nearest-neighbor coupling achieves a highly connected unit cell of 8 qubits in Chimera graph configuration. Quantum algorithms typically require coupling between arbitrary qubits. Consequently, multiple swap operations are necessary, limiting the length of quantum computation possible before processor decoherence.

Quantum bus

Another method of coupling two or more qubits is by way of a quantum bus, by pairing qubits to this intermediate. A quantum bus is often implemented as a microwave cavity modeled by a quantum harmonic oscillator. Coupled qubits may be brought in and out of resonance with the bus and with each other, eliminating the nearest-neighbor limitation. Formalism describing coupling is cavity quantum electrodynamics. In cavity quantum

electrodynamics, qubits are analogous to atoms interacting with an optical photon cavity with a difference of GHz (rather than the THz regime of electromagnetic radiation). Resonant excitation exchange among these artificial atoms is potentially useful for direct implementation of multi-qubit gates.[42] Following the dark state manifold, the Khazali-Mølmer scheme[42] performs complex multi-qubit operations in a single step, providing a substantial shortcut to the conventional circuit model.

Cross resonant gate

One popular gating mechanism uses two qubits and a bus, each tuned to different energy level separations. Applying microwave excitation to the first qubit, with a frequency resonant with the second qubit, causes a σ_x rotation of the second qubit. Rotation direction depends on the state of the first qubit, allowing a controlled phase gate construction.[43]

Following the notation of,[43] the drive Hamiltonian describing the excited system through the first qubit driving line is formally written

$$H_D/\hbar = A(t)\cos(\tilde{\omega}_2 t)\left(\sigma_x \otimes I - \frac{J}{\Delta_{12}}\sigma_z \otimes \sigma_x + m_{12} I \otimes \sigma_x\right),$$

where $A(t)$ is the shape of the microwave pulse in time, $\tilde{\omega}_2$ is resonance frequency of the second qubit, $\{I, \sigma_x, \sigma_y, \sigma_z\}$ are the Pauli matrices, J is the coupling coefficient between the two qubits via the resonator, $\Delta_{12} \equiv \omega_1 - \omega_2$ is qubit detuning, m_{12} is stray (unwanted) coupling between qubits, and $\hbar$ is Planck's constant divided by 2π. The time integral over $A(t)$ determines the angle of rotation. Unwanted rotations from the first and third terms of the Hamiltonian can be compensated for with single qubit operations. The remaining component, combined with single qubit rotations, forms a basis for the su(4) Lie algebra.

Geometric phase gate

Higher levels (outside of the computational subspace) of a pair of coupled superconducting circuits can be used to induce a geometric phase on one of the computational states of the qubits. This leads to an entangling conditional phase shift of the relevant qubit states. This effect has been implemented by flux-tuning the qubit spectra [44] and by using selective microwave driving.[45] Off-resonant driving can be used to induce differential ac-Stark shift, allowing the implementation of all-microwave controlled-phase gates.[46]

Heisenberg interactions

The Heisenberg model of interactions, written as

$$\hat{\mathcal{H}}_{\mathrm{XXZ}}/\hbar = \sum_{i,j} J_{\mathrm{XY}}(\hat{\sigma}_{\mathrm{x}}^i\hat{\sigma}_{\mathrm{x}}^j + \hat{\sigma}_{\mathrm{y}}^i\hat{\sigma}_{\mathrm{y}}^j) + J_{\mathrm{ZZ}}\hat{\sigma}_{\mathrm{z}}^i\hat{\sigma}_{\mathrm{z}}^j,$$

serves as the basis for analog quantum simulation of spin systems and the primitive for an expressive set of quantum gates, sometimes referred to as *fermionic simulation* (or *fSim*) gates. In superconducting circuits, this interaction model has been implemented using flux-tunable qubits with flux-tunable coupling,[47] allowing the demonstration of quantum supremacy.[48] In addition, it can also be realized in fixed-frequency qubits with fixed-coupling using microwave drives.[49] The fSim gate family encompasses arbitrary XY and ZZ two-qubit unitaries, including the iSWAP, the CZ, and the SWAP gates (see Quantum logic gate).

Qubit readout

Architecture-specific readout, or measurement, mechanisms exist. Readout of a phase qubit is explained in the qubit archetypes table above. A flux qubit state is often read using an adjustable DC-SQUID magnetometer. States may also be measured using an electrometer.[1] A more general readout scheme includes a coupling to a microwave resonator, where resonance frequency of the resonator is dispersively shifted by the qubit state.[50][51] Multi-level systems (qudits) can be readout using electron shelving.[52]

DiVincenzo's criteria

DiVincenzo's criteria is a list describing the requirements for a physical system to be capable of implementing a logical qubit. DiVincenzo's criteria is satisfied by superconducting quantum computing implementation. Much of the current development effort in superconducting quantum computing aim to achieve interconnect, control, and readout in the 3rd dimension with additional lithography layers.The list of DiVincenzo's criteria for a physical system to implement a logical qubit is satisfied by the implementation of superconducting qubits. Although DiVincenzo's criteria as originally proposed consists of five criteria required for physically implementing a quantum computer, the more complete list consists of seven criteria as it takes into account communication over a computer network capable of transmitting quantum information between computers, known as the “quantum internet”. Therefore, the first five criteria ensure successful quantum computing, while the final two criteria allow for quantum communication.

1. **A scalable physical system with well characterized qubits.** "Well characterized implies that that Hamiltonian function must be well-defined i.e the energy eigenstates of the qubit should be able to be quantified.. A scalable system is self-explanatory, it indicates that this ability to regulate a qubit should be augmentable for multiple more qubits. Herein lies the major issue Quantum Computers face, as more qubits are implemented it leads to a exponential increase in cost and other physical implementations which pale in comparison to the enhanced speed it may offer.[11] As superconducting qubits are fabricated on a chip, the many-qubit system is readily scalable. Qubits are allocated on the 2D surface of the chip. The demand for well characterized qubits is fulfilled with (a) qubit non-linearity (accessing only two of the available energy levels) and (b) accessing a single qubit at a time (rather than the entire many-qubit system) by way of per-qubit dedicated control lines and/or frequency separation, or tuning out, of different qubits.

2. **Ability to initialize the state of qubits to a simple fiducial state.**[53] A fiducial state is one that is easily and consistently replicable and is useful in quantum computing as it may be used to guarantee the initial state of qubits. One simple way to initialize a superconducting qubit is to wait long enough for the qubits to relax to the ground state. Controlling qubit potential with tuning knobs allows faster initialization mechanisms.
3. **Long relevant decoherence times**[53]**.** Decoherence of superconducting qubits is affected by multiple factors. Most decoherence is attributed to the quality of the Josephson junction and imperfections in the chip substrate. Due to their mesoscopic scale, superconducting qubits are relatively short lived. Nevertheless, thousands of gate operations have been demonstrated in these many-qubit systems.[54] Recent strategies to improve device coherence include purifying the circuit materials and designing qubits with decreased sensitivity to noise sources.[24]
4. **A "universal" set of quantum gates.**[53] Superconducting qubits allow arbitrary rotations in the Bloch sphere with pulsed microwave signals, implementing single qubit gates. $\sigma_z\sigma_z$ and $\sigma_x\sigma_x$ couplings are shown for most implementations and for complementing the universal gate set.[55][56][49] This criterion may also be satisfied by coupling two transmons with a coupling capacitor.[1]
5. **Qubit-specific measurement ability.**[53] In general, single superconducting qubits are used for control or for measurement.
6. **Interconvertibility of stationary and flying qubits.**[53] While stationary qubits are used to store information or perform calculations, flying qubits transmit information macroscopically. Qubits should be capable of converting from being a stationary qubit to being a flying qubit and vice versa.
7. **Reliable transmission of flying qubits between specified locations.**[53]

The final two criteria have been experimentally proven by research performed by ETH with two superconducting qubits connected by a coaxial cable.[57]

Challenges

One of the primary challenges of superconducting quantum computing is the extremely low temperatures at which superconductors like Bose-Einstein Condensates exist. Other basic challenges in superconducting qubit design are shaping the potential well and choosing particle mass such that energy separation between two specific energy levels is unique, differing from all other interlevel energy separation in the system, since these two levels are used as logical states of the qubit.

Superconducting quantum computing must also mitigate quantum noise (disruptions of the system caused by its interaction with an environment) as well as leakage (information being lost to the surrounding environment). One way to reduce leakage is with parity measurements.[16] Another strategy is to use qubits with large anharmonicity.[26][27] Many current challenges faced by superconducting quantum computing lie in the field of microwave engineering.[50] As superconducting quantum computing approaches larger scale devices, researchers face difficulties in qubit coherence, scalable calibration software, efficient determination of fidelity of quantum states across an entire chip, and qubit and gate fidelity.[16] Moreover, superconducting quantum computing devices must be reliably reproducible at increasingly large scales such that they are compatible with these improvements.[16]

The Journey of Superconducting Quantum Computing:

Although not the newest development, the focus began to shift onto superconducting qubits in the latter half of the 1990s when quantum tunneling across Josephson junctions became apparent which allowed for the realization that quantum computing could be achieved through these superconducting qubits.[58]

At the end of the century in 1999, a paper[59] was published by Yasunobu Nakamura, which exhibited the initial design of a superconducting qubit which is now known as the "charge qubit". This is the primary basis point on which later designs amended upon. These initial qubits had their limitations in respect to maintaining long coherence times and destructive measurements. The further amendment to this initial breakthrough lead to the invention of the phase and flux qubit and subsequently resulting in the transmon qubit which is now widely and primarily used in Superconducting Quantum Computing.The transmon qubit has enhanced original designs and has further cushioned charge noise from the qubit.[58]

The journey has been long, arduous and full of breakthroughs but has seen significant advancements in the recent history and has massive potential for revolutionizing computing.

The Future of Superconducting Quantum Computing:

The sector's leading industry giants, like Google, IBM and Baidu, are using superconducting quantum computing and transmon qubits to make leaps and bounds in the area of quantum computing.

In August 2022, Baidu released its plans to build a fully integrated top to bottom quantum computer which incorporated superconducting qubits. This computer will be all encompassing with hardware, software and applications fully integrated. This is a first in the world of quantum computing and will lead to ground-breaking advancements.[60]

IBM released the following roadmap publicly that they have set for their quantum computers which also incorporated superconducting qubits and the transmon qubit.

2021: In 2021, IBM came out with their 127-qubit processor.[61]

2022: On November 9, IBM announced its 433 qubit processor called "Osprey".[62]

2023: IBM plan on releasing their Condor quantum processor with 1,121 qubits.[61]

2024: IBM plan on releasing their Flamingo quantum processor with 1,386+ qubits.[61]

2025: IBM plan on releasing their Kookaburra quantum processor with 4,158+ qubits.[61]

2026 and beyond: IBM plan on releasing a quantum processor that scaled beyond 10,000 qubits to a 100,000 qubits.[61]

Google in 2016, implemented 16 qubits to convey a demonstration of the Fermi-Hubbard Model. In another recent experiment, Google used 17 qubits to optimize the Sherrington-Kirkpatrick model. Google produced the Sycamore quantum computer which performed a task in 200 seconds that would have taken 10,000 years on a classical computer.[63]

References

1. "PennyLane Documentation — PennyLane" (https://docs.pennylane.ai/en/stable/index.html). *docs.pennylane.ai*. Retrieved 2022-12-11.
2. Castelvecchi, Davide (5 January 2017). "Quantum computers ready to leap out of the lab in 2017" (https://doi.org/10.1038%2F541009a). *Nature*. **541** (7635): 9–10. Bibcode:2017Natur.541....9C (https://ui.adsabs.harvard.edu/abs/2017Natur.541....9C). doi:10.1038/541009a (https://doi.org/10.1038%2F541009a). PMID 28054624 (https://pubmed.ncbi.nlm.nih.gov/28054624). S2CID 4447373 (https://api.semanticscholar.org/CorpusID:4447373).
3. "IBM Makes Quantum Computing Available on IBM Cloud" (https://web.archive.org/web/20160504214945/http://www-03.ibm.com/press/us/en/pressrelease/49661.wss). *www-03.ibm.com*. 4 May 2016. Archived from the original (https://www-03.ibm.com/press/us/en/pressrelease/49661.wss) on May 4, 2016.
4. "Imec enters the race to unleash quantum computing with silicon qubits" (https://www.imec-int.com/en/articles/imec-enters-the-race-to-unleash-quantum-computing-with-silicon-qubits). *www.imec-int.com*. Retrieved 2019-11-10.
5. Colm A. Ryan, Blake R. Johnson, Diego Ristè, Brian Donovan, Thomas A. Ohki, "Hardware for Dynamic Quantum Computing", arXiv:1704.08314v1
6. "Rigetti Launches Quantum Cloud Services, Announces $1Million Challenge" (https://www.hpcwire.com/2018/09/07/rigetti-launches-quantum-cloud-services-announces-1million-challenge/). *HPCwire*. 2018-09-07. Retrieved 2018-09-16.
7. "Intel Invests US$50 Million to Advance Quantum Computing | Intel Newsroom" (https://newsroom.intel.com/news-releases/intel-invests-us50-million-to-advance-quantum-computing/). *Intel Newsroom*.
8. Kelly, J.; Barends, R.; Fowler, A. G.; Megrant, A.; Jeffrey, E.; White, T. C.; Sank, D.; Mutus, J. Y.; Campbell, B.; Chen, Yu; Chen, Z.; Chiaro, B.; Dunsworth, A.; Hoi, I.-C.; Neill, C.; O'Malley, P. J. J.; Quintana, C.; Roushan, P.; Vainsencher, A.; Wenner, J.; Cleland, A. N.; Martinis, John M. (4 March 2015). "State preservation by repetitive error detection in a superconducting quantum circuit". *Nature*. **519** (7541): 66–69. arXiv:1411.7403 (https://arxiv.org/abs/1411.7403). Bibcode:2015Natur.519...66K (https://ui.adsabs.harvard.edu/abs/2015Natur.519...66K). doi:10.1038/nature14270 (https://doi.org/10.1038%2Fnature14270). PMID 25739628 (https://pubmed.ncbi.nlm.nih.gov/25739628). S2CID 3032369 (https://api.semanticscholar.org/CorpusID:3032369).
9. Arute, Frank; Arya, Kunal; Babbush, Ryan; Bacon, Dave; Bardin, Joseph C.; Barends, Rami; Biswas, Rupak; Boixo, Sergio; Brandao, Fernando G. S. L.; Buell, David A.; Burkett, Brian; Chen, Yu; Chen, Zijun; Chiaro, Ben; Collins, Roberto; Courtney, William; Dunsworth, Andrew; Farhi, Edward; Foxen, Brooks; Fowler, Austin; Gidney, Craig; Giustina, Marissa; Graff, Rob; Guerin, Keith; Habegger, Steve; Harrigan, Matthew P.; Hartmann, Michael J.; Ho, Alan; Hoffmann, Markus; Huang, Trent; Humble, Travis S.; Isakov, Sergei V.; Jeffrey, Evan; Jiang, Zhang; Kafri, Dvir; Kechedzhi, Kostyantyn; Kelly, Julian; Klimov, Paul V.; Knysh, Sergey; Korotkov, Alexander; Kostritsa, Fedor; Landhuis, David; Lindmark, Mike; Lucero, Erik; Lyakh, Dmitry; Mandrà, Salvatore; McClean, Jarrod R.; McEwen, Matthew; Megrant, Anthony; Mi, Xiao; Michielsen, Kristel; Mohseni, Masoud; Mutus, Josh; Naaman, Ofer; Neeley, Matthew; Neill, Charles; Niu, Murphy Yuezhen; Ostby, Eric; Petukhov, Andre; Platt, John C.; Quintana, Chris; Rieffel, Eleanor G.; Roushan, Pedram; Rubin, Nicholas C.; Sank, Daniel; Satzinger, Kevin J.; Smelyanskiy, Vadim; Sung, Kevin J.; Trevithick, Matthew D.; Vainsencher, Amit; Villalonga, Benjamin; White, Theodore; Yao, Z. Jamie; Yeh, Ping; Zalcman, Adam; Neven, Hartmut; Martinis, John M. (October 2019). "Quantum supremacy using a programmable superconducting processor" (https://doi.org/10.1038%2Fs41586-019-1666-5). *Nature*. **574** (7779): 505–510. arXiv:1910.11333 (https://arxiv.org/abs/1910.11333). Bibcode:2019Natur.574..505A (https://ui.adsabs.harvard.edu/abs/2019Natur.574..505A). doi:10.1038/s41586-019-1666-5 (https://doi.org/10.1038%2Fs41586-019-1666-5). PMID 31645734 (https://pubmed.ncbi.nlm.nih.gov/31645734).
10. Dayal, Geeta. "LEGO Turing Machine Is Simple, Yet Sublime" (https://www.wired.com/2012/06/lego-turing-machine/). *WIRED*.
11. "DiVincenzo's Criteria - Quantum Computing Codex" (https://qc-at-davis.github.io/QCC/How-Quantum-Computing-Works/DiVincenzo%27s-Criteria/DiVincenzo%27s-Criteria.html#initialize-the-state-of-qubits-to-a-simple-fiducial-state). *qc-at-davis.github.io*. Retrieved 2022-12-13.
12. Ballon, Alvaro (22 March 2022). "Quantum computing with superconducting qubits — PennyLane" (https://pennylane.ai/qml/demos/tutorial_sc_qubits.html). *Pennylane Demos*. Retrieved 2022-12-13.
13. "Cooper Pairs" (http://hyperphysics.phy-astr.gsu.edu/hbase/Solids/coop.html).
14. Shen, L. Y. L. (1972-02-01). "Superconductivity of Tantalum, Niobium and Lanthanum Studied by Electron Tunneling: Problems of Surface Contamination" (https://aip.scitation.org/doi/abs/10.1063/1.2946195). *AIP Conference Proceedings*. **4** (1): 31–44. Bibcode:1972AIPC....4...31S (https://ui.adsabs.harvard.edu/abs/1972AIPC....4...31S). doi:10.1063/1.2946195 (https://doi.org/10.1063%2F1.2946195). ISSN 0094-243X (https://search.worldcat.org/issn/0094-243X).
15. Greicius, Tony (2020-06-12). "NASA's Cold Atom Lab Takes One Giant Leap for Quantum Science" (http://www.nasa.gov/feature/jpl/nasas-cold-atom-lab-takes-one-giant-leap-for-quantum-science). *NASA*. Retrieved 2022-12-11.
16. Kjaergaard, Morten; Schwartz, Mollie E.; Braumüller, Jochen; Krantz, Philip; Wang, Joel I.-Jan; Gustavsson, Simon; Oliver, William D. (2020-03-10). "Superconducting Qubits: Current State of Play". *Annual Review of Condensed Matter Physics*. **11** (1): 369–395. arXiv:1905.13641 (https://arxiv.org/abs/1905.13641). Bibcode:2020ARCMP..11..369K (https://ui.adsabs.harvard.edu/abs/2020ARCMP..11..369K). doi:10.1146/annurev-conmatphys-031119-050605 (https://doi.org/10.1146%2Fannurev-conmatphys-031119-050605). ISSN 1947-5454 (https://search.worldcat.org/issn/1947-5454). S2CID 173188891 (https://api.semanticscholar.org/CorpusID:173188891).
17. Manucharyan, V. E.; Koch, J.; Glazman, L. I.; Devoret, M. H. (1 October 2009). "Fluxonium: Single Cooper-Pair Circuit Free of Charge Offsets". *Science*. **326** (5949): 113–116. arXiv:0906.0831 (https://arxiv.org/abs/0906.0831). Bibcode:2009Sci...326..113M (https://ui.adsabs.harvard.edu/abs/2009Sci...326..113M). doi:10.1126/science.1175552 (https://doi.org/10.1126%2Fscience.1175552). PMID 19797655 (https://pubmed.ncbi.nlm.nih.gov/19797655). S2CID 17645288 (https://api.semanticscholar.org/CorpusID:17645288).

18. Houck, A. A.; Koch, Jens; Devoret, M. H.; Girvin, S. M.; Schoelkopf, R. J. (11 February 2009). "Life after charge noise: recent results with transmon qubits". *Quantum Information Processing*. **8** (2–3): 105–115. arXiv:0812.1865 (https://arxiv.org/abs/0812.1865). doi:10.1007/s11128-009-0100-6 (https://doi.org/10.1007%2Fs11128-009-0100-6). S2CID 27305073 (https://api.semanticscholar.org/CorpusID:27305073).
19. Barends, R.; Kelly, J.; Megrant, A.; Sank, D.; Jeffrey, E.; Chen, Y.; Yin, Y.; Chiaro, B.; Mutus, J.; Neill, C.; O'Malley, P.; Roushan, P.; Wenner, J.; White, T. C.; Cleland, A. N.; Martinis, John M. (22 August 2013). "Coherent Josephson Qubit Suitable for Scalable Quantum Integrated Circuits". *Physical Review Letters*. **111** (8): 080502. arXiv:1304.2322 (https://arxiv.org/abs/1304.2322). Bibcode:2013PhRvL.111h0502B (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111h0502B). doi:10.1103/PhysRevLett.111.080502 (https://doi.org/10.1103%2FPhysRevLett.111.080502). PMID 24010421 (https://pubmed.ncbi.nlm.nih.gov/24010421). S2CID 27081288 (https://api.semanticscholar.org/CorpusID:27081288).
20. Metcalfe, M.; Boaknin, E.; Manucharyan, V.; Vijay, R.; Siddiqi, I.; Rigetti, C.; Frunzio, L.; Schoelkopf, R. J.; Devoret, M. H. (21 November 2007). "Measuring the decoherence of a quantronium qubit with the cavity bifurcation amplifier". *Physical Review B*. **76** (17): 174516. arXiv:0706.0765 (https://arxiv.org/abs/0706.0765). Bibcode:2007PhRvB..76q4516M (https://ui.adsabs.harvard.edu/abs/2007PhRvB..76q4516M). doi:10.1103/PhysRevB.76.174516 (https://doi.org/10.1103%2FPhysRevB.76.174516). S2CID 19088840 (https://api.semanticscholar.org/CorpusID:19088840).
21. Martinis, John M.; Osborne, Kevin (2004-02-16). "Superconducting Qubits and the Physics of Josephson Junctions". arXiv:cond-mat/0402415 (https://arxiv.org/abs/cond-mat/0402415). Bibcode:2004cond.mat..2415M (https://ui.adsabs.harvard.edu/abs/2004cond.mat..2415M). {{cite journal}}: Cite journal requires |journal= (help)
22. Hyyppä, Eric; Kundu, Suman; Chan, Chun Fai; Gunyhó, András; Hotari, Juho; Janzso, David; Juliusson, Kristinn; Kiuru, Olavi; Kotilahti, Janne; Landra, Alessandro; Liu, Wei; Marxer, Fabian; Mäkinen, Akseli; Orgiazzi, Jean-Luc; Palma, Mario (2022-11-12). "Unimon qubit" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9653402). *Nature Communications*. **13** (1): 6895. arXiv:2203.05896 (https://arxiv.org/abs/2203.05896). Bibcode:2022NatCo..13.6895H (https://ui.adsabs.harvard.edu/abs/2022NatCo..13.6895H). doi:10.1038/s41467-022-34614-w (https://doi.org/10.1038%2Fs41467-022-34614-w). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 9653402 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9653402). PMID 36371435 (https://pubmed.ncbi.nlm.nih.gov/36371435).
23. Cottet, Nathanaël; Xiong, Haonan; Nguyen, Long B.; Lin, Yen-Hsiang; Manucharyan, Vladimir E. (2021-11-04). "Electron shelving of a superconducting artificial atom" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8569191). *Nature Communications*. **12** (1): 6383. arXiv:2008.02423 (https://arxiv.org/abs/2008.02423). Bibcode:2021NatCo..12.6383C (https://ui.adsabs.harvard.edu/abs/2021NatCo..12.6383C). doi:10.1038/s41467-021-26686-x (https://doi.org/10.1038%2Fs41467-021-26686-x). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 8569191 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8569191). PMID 34737313 (https://pubmed.ncbi.nlm.nih.gov/34737313).
24. Nguyen, Long B.; Lin, Yen-Hsiang; Somoroff, Aaron; Mencia, Raymond; Grabon, Nicholas; Manucharyan, Vladimir E. (25 November 2019). "High-Coherence Fluxonium Qubit" (https://link.aps.org/doi/10.1103/PhysRevX.9.041041). *Physical Review X*. **9** (4): 041041. arXiv:1810.11006 (https://arxiv.org/abs/1810.11006). Bibcode:2019PhRvX...9d1041N (https://ui.adsabs.harvard.edu/abs/2019PhRvX...9d1041N). doi:10.1103/PhysRevX.9.041041 (https://doi.org/10.1103%2FPhysRevX.9.041041). ISSN 2160-3308 (https://search.worldcat.org/issn/2160-3308). S2CID 53499609 (https://api.semanticscholar.org/CorpusID:53499609).
25. Science, The National University of; MISIS, Technology. "Fluxonium qubits bring the creation of a quantum computer closer" (https://phys.org/news/2022-11-fluxonium-qubits-creation-quantum-closer.html). *phys.org*. Retrieved 2022-12-12.
26. Nguyen, Long B. (2020). *Toward the Fluxonium Quantum Processor* (https://www.proquest.com/dissertations-theses/toward-fluxonium-quantum-processor/docview/2455525166/se-2) (Ph.D. thesis). University of Maryland, College Park.
27. Nguyen, Long B.; Koolstra, Gerwin; Kim, Yosep; Morvan, Alexis; Chistolini, Trevor; Singh, Shraddha; Nesterov, Konstantin N.; Jünger, Christian; Chen, Larry; Pedramrazi, Zahra; Mitchell, Bradley K.; Kreikebaum, John Mark; Puri, Shruti; Santiago, David I.; Siddiqi, Irfan (5 August 2022). "Blueprint for a High-Performance Fluxonium Quantum Processor" (https://link.aps.org/doi/10.1103/PRXQuantum.3.037001). *PRX Quantum*. **3** (3): 037001. arXiv:2201.09374 (https://arxiv.org/abs/2201.09374). Bibcode:2022PRXQ....3c7001N (https://ui.adsabs.harvard.edu/abs/2022PRXQ....3c7001N). doi:10.1103/PRXQuantum.3.037001 (https://doi.org/10.1103%2FPRXQuantum.3.037001).
28. "Superconducting qubits – on islands, charge qubits and the transmon" (https://leftasexercise.com/2019/06/06/superconducting-qubits-on-islands-charge-qubits-and-the-transmon/). *LeftAsExercise*. 2019-06-06. Retrieved 2022-12-12.
29. Wendin, G. (2017-10-01). "Quantum information processing with superconducting circuits: a review". *Reports on Progress in Physics*. **80** (10): 106001. arXiv:1610.02208 (https://arxiv.org/abs/1610.02208). Bibcode:2017RPPh...80j6001W (https://ui.adsabs.harvard.edu/abs/2017RPPh...80j6001W). doi:10.1088/1361-6633/aa7e1a (https://doi.org/10.1088%2F1361-6633%2Faa7e1a). ISSN 0034-4885 (https://search.worldcat.org/issn/0034-4885). PMID 28682303 (https://pubmed.ncbi.nlm.nih.gov/28682303). S2CID 3940479 (https://api.semanticscholar.org/CorpusID:3940479).
30. Gambetta, J. M.; Chow, J. M.; Steffen, M. (2017). "Building logical qubits in a superconducting quantum computing system" (https://doi.org/10.1038%2Fs41534-016-0004-0). *npj Quantum Information*. **3** (1): 2. arXiv:1510.04375 (https://arxiv.org/abs/1510.04375). Bibcode:2017npjQI...3....2G (https://ui.adsabs.harvard.edu/abs/2017npjQI...3....2G). doi:10.1038/s41534-016-0004-0 (https://doi.org/10.1038%2Fs41534-016-0004-0).
31. Roth, Thomas E.; Ma, Ruichao; Chew, Weng C. (2021-06-21). "An Introduction to the Transmon Qubit for Electromagnetic Engineers". arXiv:2106.11352 (https://arxiv.org/abs/2106.11352). {{cite journal}}: Cite journal requires |journal= (help)
32. Kjaergaard, Morten; Schwartz, Mollie E.; Braumüller, Jochen; Krantz, Philip; Wang, Joel I.-J.; Gustavsson, Simon; Oliver, William D. (2020-03-10). "Superconducting Qubits: Current State of Play" (https://www.annualreviews.org/doi/10.1146/annurev-conmatphys-031119-050605). *Annual Review of Condensed Matter Physics*. **11** (1): 369–395. arXiv:1905.13641 (https://arxiv.org/abs/1905.13641). Bibcode:2020ARCMP..11..369K (https://ui.adsabs.harvard.edu/abs/2020ARCMP..11..369K). doi:10.1146/annurev-conmatphys-031119-050605 (https://doi.org/10.1146%2Fannurev-conmatphys-031119-050605). ISSN 1947-5454 (https://search.worldcat.org/issn/1947-5454). S2CID 173188891 (https://api.semanticscholar.org/CorpusID:173188891).
33. Shim, Yun-Pil; Tahan, Charles (2016-03-17). "Semiconductor-inspired design principles for superconducting quantum computing" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4800439). *Nature Communications*. **7** (1): 11059. arXiv:1507.07923 (https://arxiv.org/abs/1507.07923). Bibcode:2016NatCo...711059S (https://ui.adsabs.harvard.edu/abs/2016NatCo...711059S). doi:10.1038/ncomms11059 (https://doi.org/10.1038%2Fncomms11059). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 4800439 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4800439). PMID 26983379 (https://pubmed.ncbi.nlm.nih.gov/26983379).

34. Wang, Chenlu; Li, Xuegang; Xu, Huikai; Li, Zhiyuan; Wang, Junhua; Yang, Zhen; Mi, Zhenyu; Liang, Xuehui; Su, Tang; Yang, Chuhong; Wang, Guangyue; Wang, Wenyan; Li, Yongchao; Chen, Mo; Li, Chengyao (2022-01-13). "Towards practical quantum computers: transmon qubit with a lifetime approaching 0.5 milliseconds" (https://www.nature.com/articles/s41534-021-00510-2). *npj Quantum Information*. **8** (1): 3. arXiv:2105.09890 (https://arxiv.org/abs/2105.09890). Bibcode:2022npjQI...8....3W (https://ui.adsabs.harvard.edu/abs/2022npjQI...8....3W). doi:10.1038/s41534-021-00510-2 (https://doi.org/10.1038%2Fs41534-021-00510-2). ISSN 2056-6387 (https://search.worldcat.org/issn/2056-6387). S2CID 245950831 (https://api.semanticscholar.org/CorpusID:245950831).
35. "Fig. 1: Unimon qubit and its measurement setup. | Nature Communications" (https://www.nature.com/articles/s41467-022-34614-w/figures/1). {{cite journal}}: Cite journal requires |journal= (help)
36. "Unimon: A new qubit to boost quantum computers from IQM | IQM" (https://www.meetiqm.com/articles/press-releases/iqm-unimon-qubit/). *www.meetiqm.com*. Retrieved 2022-12-12.
37. Buchanan, Mark (2022-12-08). "Meet the Unimon, the New Qubit on the Block" (https://physics.aps.org/articles/v15/191). *Physics*. **15**: 191. Bibcode:2022PhyOJ..15..191B (https://ui.adsabs.harvard.edu/abs/2022PhyOJ..15..191B). doi:10.1103/Physics.15.191 (https://doi.org/10.1103%2FPhysics.15.191). S2CID 257514449 (https://api.semanticscholar.org/CorpusID:257514449).
38. Devoret, M. H.; Wallraff, A.; Martinis, J. M. (6 November 2004). "Superconducting Qubits: A Short Review". arXiv:cond-mat/0411174 (https://arxiv.org/abs/cond-mat/0411174).
39. Motzoi, F.; Gambetta, J. M.; Rebentrost, P.; Wilhelm, F. K. (8 September 2009). "Simple Pulses for Elimination of Leakage in Weakly Nonlinear Qubits". *Physical Review Letters*. **103** (11): 110501. arXiv:0901.0534 (https://arxiv.org/abs/0901.0534). Bibcode:2009PhRvL.103k0501M (https://ui.adsabs.harvard.edu/abs/2009PhRvL.103k0501M). doi:10.1103/PhysRevLett.103.110501 (https://doi.org/10.1103%2FPhysRevLett.103.110501). PMID 19792356 (https://pubmed.ncbi.nlm.nih.gov/19792356). S2CID 7288207 (https://api.semanticscholar.org/CorpusID:7288207).
40. Chuang, Michael A. Nielsen & Isaac L. (2010). *Quantum computation and quantum information* (https://archive.org/details/quantumcomputati00niel) (10th anniversary ed.). Cambridge: Cambridge University Press. pp. 174 (https://archive.org/details/quantumcomputati00niel/page/n207)–176. ISBN 978-1-107-00217-3.
41. Rigetti, Chad Tyler (2009). *Quantum gates for superconducting qubits*. p. 21. Bibcode:2009PhDT.....50R (https://ui.adsabs.harvard.edu/abs/2009PhDT.....50R). ISBN 9781109198874.
42. Khazali, Mohammadsadegh; Mølmer, Klaus (2020-06-11). "Fast Multiqubit Gates by Adiabatic Evolution in Interacting Excited-State Manifolds of Rydberg Atoms and Superconducting Circuits" (https://doi.org/10.1103%2FPhysRevX.10.021054). *Physical Review X*. **10** (2): 021054. arXiv:2006.07035 (https://arxiv.org/abs/2006.07035). Bibcode:2020PhRvX..10b1054K (https://ui.adsabs.harvard.edu/abs/2020PhRvX..10b1054K). doi:10.1103/PhysRevX.10.021054 (https://doi.org/10.1103%2FPhysRevX.10.021054). ISSN 2160-3308 (https://search.worldcat.org/issn/2160-3308).
43. Chow, Jerry M.; Córcoles, A. D.; Gambetta, Jay M.; Rigetti, Chad; Johnson, B. R.; Smolin, John A.; Rozen, J. R.; Keefe, George A.; Rothwell, Mary B.; Ketchen, Mark B.; Steffen, M. (17 August 2011). "Simple All-Microwave Entangling Gate for Fixed-Frequency Superconducting Qubits". *Physical Review Letters*. **107** (8): 080502. arXiv:1106.0553 (https://arxiv.org/abs/1106.0553). Bibcode:2011PhRvL.107h0502C (https://ui.adsabs.harvard.edu/abs/2011PhRvL.107h0502C). doi:10.1103/PhysRevLett.107.080502 (https://doi.org/10.1103%2FPhysRevLett.107.080502). PMID 21929152 (https://pubmed.ncbi.nlm.nih.gov/21929152). S2CID 9302474 (https://api.semanticscholar.org/CorpusID:9302474).
44. DiCarlo, L.; Chow, J. M.; Gambetta, J. M.; Bishop, Lev S.; Johnson, B. R.; Schuster, D. I.; Majer, J.; Blais, A.; Frunzio, L.; Girvin, S. M.; Schoelkopf, R. J. (2009-06-28). "Demonstration of two-qubit algorithms with a superconducting quantum processor". *Nature*. **460** (7252). Springer Science and Business Media LLC: 240–244. doi:10.1038/nature08121 (https://doi.org/10.1038%2Fnature08121). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836).
45. Ficheux, Quentin; Nguyen, Long B.; Somoroff, Aaron; Xiong, Haonan; Nesterov, Konstantin N.; Vavilov, Maxim G.; Manucharyan, Vladimir E. (2021-05-03). "Fast Logic with Slow Qubits: Microwave-Activated Controlled-Z Gate on Low-Frequency Fluxoniums". *Physical Review X*. **11** (2). arXiv:2011.02634 (https://arxiv.org/abs/2011.02634). doi:10.1103/PhysRevX.11.021026 (https://doi.org/10.1103%2FPhysRevX.11.021026). ISSN 2160-3308 (https://search.worldcat.org/issn/2160-3308).
46. Xiong, Haonan; Ficheux, Quentin; Somoroff, Aaron; Nguyen, Long B.; Dogan, Ebru; Rosenstock, Dario; Wang, Chen; Nesterov, Konstantin N.; Vavilov, Maxim G.; Manucharyan, Vladimir E. (2022-04-15). "Arbitrary controlled-phase gate on fluxonium qubits using differential ac Stark shifts". *Physical Review Research*. **4** (2). arXiv:2103.04491 (https://arxiv.org/abs/2103.04491). doi:10.1103/PhysRevResearch.4.023040 (https://doi.org/10.1103%2FPhysRevResearch.4.023040). ISSN 2643-1564 (https://search.worldcat.org/issn/2643-1564).
47. Foxen, B.; Neill, C.; Dunsworth, A.; Roushan, P.; Chiaro, B.; Megrant, A.; Kelly, J.; Chen, Zijun; Satzinger, K.; Barends, R.; Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J. C.; Boixo, S.; Buell, D.; Burkett, B.; Chen, Yu; Collins, R.; Farhi, E.; Fowler, A.; Gidney, C.; Giustina, M.; Graff, R.; Harrigan, M.; Huang, T.; Isakov, S. V.; Jeffrey, E.; Jiang, Z.; Kafri, D.; Kechedzhi, K.; Klimov, P.; Korotkov, A.; Kostritsa, F.; Landhuis, D.; Lucero, E.; McClean, J.; McEwen, M.; Mi, X.; Mohseni, M.; Mutus, J. Y.; Naaman, O.; Neeley, M.; Niu, M.; Petukhov, A.; Quintana, C.; Rubin, N.; Sank, D.; Smelyanskiy, V.; Vainsencher, A.; White, T. C.; Yao, Z.; Yeh, P.; Zalcman, A.; Neven, H.; Martinis, J. M.; Google AI Quantum (2020-09-15). "Demonstrating a Continuous Set of Two-qubit Gates for Near-term Quantum Algorithms". *Physical Review Letters*. **125** (12). arXiv:2001.08343 (https://arxiv.org/abs/2001.08343). doi:10.1103/PhysRevLett.125.120504 (https://doi.org/10.1103%2FPhysRevLett.125.120504). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). {{cite journal}}: |author58= has generic name (help)
48. Arute, Frank; Arya, Kunal; Babbush, Ryan; Bacon, Dave; Bardin, Joseph C.; Barends, Rami; Biswas, Rupak; Boixo, Sergio; Brandao, Fernando G. S. L.; Buell, David A.; Burkett, Brian; Chen, Yu; Chen, Zijun; Chiaro, Ben; Collins, Roberto; Courtney, William; Dunsworth, Andrew; Farhi, Edward; Foxen, Brooks; Fowler, Austin; Gidney, Craig; Giustina, Marissa; Graff, Rob; Guerin, Keith; Habegger, Steve; Harrigan, Matthew P.; Hartmann, Michael J.; Ho, Alan; Hoffmann, Markus; Huang, Trent; Humble, Travis S.; Isakov, Sergei V.; Jeffrey, Evan; Jiang, Zhang; Kafri, Dvir; Kechedzhi, Kostyantyn; Kelly, Julian; Klimov, Paul V.; Knysh, Sergey; Korotkov, Alexander; Kostritsa, Fedor; Landhuis, David; Lindmark, Mike; Lucero, Erik; Lyakh, Dmitry; Mandrà, Salvatore; McClean, Jarrod R.; McEwen, Matthew; Megrant, Anthony; Mi, Xiao; Michielsen, Kristel; Mohseni, Masoud; Mutus, Josh; Naaman, Ofer; Neeley, Matthew; Neill, Charles; Niu, Murphy Yuezhen; Ostby, Eric; Petukhov, Andre; Platt, John C.; Quintana, Chris; Rieffel, Eleanor G.; Roushan, Pedram; Rubin, Nicholas C.; Sank, Daniel; Satzinger, Kevin J.; Smelyanskiy, Vadim; Sung, Kevin J.; Trevithick, Matthew D.; Vainsencher, Amit; Villalonga, Benjamin; White, Theodore; Yao, Z. Jamie; Yeh, Ping; Zalcman, Adam; Neven, Hartmut; Martinis, John M. (2019-10-23). "Quantum supremacy using a programmable superconducting processor". *Nature*. **574** (7779). Springer Science and Business Media LLC: 505–510. arXiv:1910.11333 (https://arxiv.org/abs/1910.11333). doi:10.1038/s41586-019-1666-5 (https://doi.org/10.1038%2Fs41586-019-1666-5). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836).

49. Nguyen, L.B.; Kim, Y.; Hashim, A.; Goss, N.; Marinelli, B.; Bhandari, B.; Das, D.; Naik, R.K.; Kreikebaum, J.M.; Jordan, A.; Santiago, D.I.; Siddiqi, I. (16 January 2024). "Programmable Heisenberg interactions between Floquet qubits" (https://doi.org/10.1038%2Fs41567-023-02326-7). *Nature Physics*. **20** (1): 240–246. arXiv:2211.10383 (https://arxiv.org/abs/2211.10383). Bibcode:2024NatPh..20..240N (https://ui.adsabs.harvard.edu/abs/2024NatPh..20..240N). doi:10.1038/s41567-023-02326-7 (https://doi.org/10.1038%2Fs41567-023-02326-7).
50. Gambetta, Jay M.; Chow, Jerry M.; Steffen, Matthias (13 January 2017). "Building logical qubits in a superconducting quantum computing system" (https://doi.org/10.1038%2Fs41534-016-0004-0). *npj Quantum Information*. **3** (1): 2. arXiv:1510.04375 (https://arxiv.org/abs/1510.04375). Bibcode:2017npjQI...3....2G (https://ui.adsabs.harvard.edu/abs/2017npjQI...3....2G). doi:10.1038/s41534-016-0004-0 (https://doi.org/10.1038%2Fs41534-016-0004-0).
51. Blais, Alexandre; Huang, Ren-Shou; Wallraff, Andreas; Girvin, Steven; Schoelkopf, Robert (2004). "Cavity quantum electrodynamics for superconducting electrical circuits: An architecture for quantum computation" (https://link.aps.org/doi/10.1103/PhysRevA.69.062320). *Phys. Rev. A*. **69** (6): 062320. arXiv:cond-mat/0402216 (https://arxiv.org/abs/cond-mat/0402216). Bibcode:2004PhRvA..69f2320B (https://ui.adsabs.harvard.edu/abs/2004PhRvA..69f2320B). doi:10.1103/PhysRevA.69.062320 (https://doi.org/10.1103%2FPhysRevA.69.062320). S2CID 20427333 (https://api.semanticscholar.org/CorpusID:20427333).
52. Cottet, Nathanaël; Xiong, Haonan; Nguyen, Long B.; Lin, Yen-Hsiang; Manucharyan, Vladimir E. (2021-11-04). "Electron shelving of a superconducting artificial atom". *Nature Communications*. **12** (1). Springer Science and Business Media LLC. arXiv:2008.02423 (https://arxiv.org/abs/2008.02423). doi:10.1038/s41467-021-26686-x (https://doi.org/10.1038%2Fs41467-021-26686-x). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723).
53. DiVincenzo, David (February 1, 2008). "The Physical Implementation of Quantum Computation". *IBM T.J. Watson Research Center*. **48** (9–11): 771–783. arXiv:quant-ph/0002077 (https://arxiv.org/abs/quant-ph/0002077). Bibcode:2000ForPh..48..771D (https://ui.adsabs.harvard.edu/abs/2000ForPh..48..771D). doi:10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E (https://doi.org/10.1002%2F1521-3978%28200009%2948%3A9%2F11%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E). S2CID 15439711 (https://api.semanticscholar.org/CorpusID:15439711).
54. Devoret, M. H.; Schoelkopf, R. J. (7 March 2013). "Superconducting Circuits for Quantum Information: An Outlook". *Science*. **339** (6124): 1169–1174. Bibcode:2013Sci...339.1169D (https://ui.adsabs.harvard.edu/abs/2013Sci...339.1169D). doi:10.1126/science.1231930 (https://doi.org/10.1126%2Fscience.1231930). PMID 23471399 (https://pubmed.ncbi.nlm.nih.gov/23471399). S2CID 10123022 (https://api.semanticscholar.org/CorpusID:10123022).
55. Chow, Jerry M.; Gambetta, Jay M.; Córcoles, A. D.; Merkel, Seth T.; Smolin, John A.; Rigetti, Chad; Poletto, S.; Keefe, George A.; Rothwell, Mary B.; Rozen, J. R.; Ketchen, Mark B.; Steffen, M. (9 August 2012). "Universal Quantum Gate Set Approaching Fault-Tolerant Thresholds with Superconducting Qubits". *Physical Review Letters*. **109** (6): 060501. arXiv:1202.5344 (https://arxiv.org/abs/1202.5344). Bibcode:2012PhRvL.109f0501C (https://ui.adsabs.harvard.edu/abs/2012PhRvL.109f0501C). doi:10.1103/PhysRevLett.109.060501 (https://doi.org/10.1103%2FPhysRevLett.109.060501). PMID 23006254 (https://pubmed.ncbi.nlm.nih.gov/23006254). S2CID 39874288 (https://api.semanticscholar.org/CorpusID:39874288).
56. Niskanen, A. O.; Harrabi, K.; Yoshihara, F.; Nakamura, Y.; Lloyd, S.; Tsai, J. S. (4 May 2007). "Quantum Coherent Tunable Coupling of Superconducting Qubits". *Science*. **316** (5825): 723–726. Bibcode:2007Sci...316..723N (https://ui.adsabs.harvard.edu/abs/2007Sci...316..723N). doi:10.1126/science.1141324 (https://doi.org/10.1126%2Fscience.1141324). PMID 17478714 (https://pubmed.ncbi.nlm.nih.gov/17478714). S2CID 43175104 (https://api.semanticscholar.org/CorpusID:43175104).
57. Morsch, Oliver; Zurich, E. T. H. "Quantum transfer at the push of a button" (https://phys.org/news/2018-06-quantum-button.html). *phys.org*. Retrieved 2022-12-09.
58. Qiskit (2022-09-28). "How The First Superconducting Qubit Changed Quantum Computing Forever" (https://medium.com/qiskit/how-the-first-superconducting-qubit-changed-quantum-computing-forever-96cf261b8498). *Qiskit*. Retrieved 2022-12-13.
59. Nakamura, Y.; Pashkin, Yu A.; Tsai, J. S. (April 1999). "Coherent control of macroscopic quantum states in a single-Cooper-pair box". *Nature*. **398** (6730): 786–788. arXiv:cond-mat/9904003 (https://arxiv.org/abs/cond-mat/9904003). Bibcode:1999Natur.398..786N (https://ui.adsabs.harvard.edu/abs/1999Natur.398..786N). doi:10.1038/19718 (https://doi.org/10.1038%2F19718). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). S2CID 4392755 (https://api.semanticscholar.org/CorpusID:4392755).
60. "Baidu Releases Superconducting Quantum Computer and World's First All-Platform Integration Solution, Making Quantum Computing Within Reach" (https://www.prnewswire.com/news-releases/baidu-releases-superconducting-quantum-computer-and-worlds-first-all-platform-integration-solution-making-quantum-computing-within-reach-301612321.html). *www.prnewswire.com* (Press release). Retrieved 2022-12-13.
61. "IBM Quantum roadmap to build quantum-centric supercomputers" (https://research.ibm.com/blog/ibm-quantum-roadmap-2025). *IBM Research Blog*. 2021-02-09. Retrieved 2022-12-13.
62. Lardinois, Frederic (2022-11-09). "IBM unveils its 433 qubit Osprey quantum computer" (https://techcrunch.com/2022/11/09/ibm-unveils-its-433-qubit-osprey-quantum-computer/). *TechCrunch*. Retrieved 2022-12-13.
63. "Our quantum computing journey" (https://dreamcoat-guggenheim.uc.r.appspot.com/learn/map/). *Google Quantum AI*. Retrieved 2022-12-13.

Further reading

- Stancil, Daniel D.; Byrd, Gregory T. (2022). *Principles of Superconducting Quantum Computers* (1st ed.). Hoboken, New Jersey: John Wiley & Sons. ISBN 978-1-119-75072-7. OCLC 1302334194 (https://search.worldcat.org/oclc/1302334194). 978-1-119-75074-1 (ebook).

External links

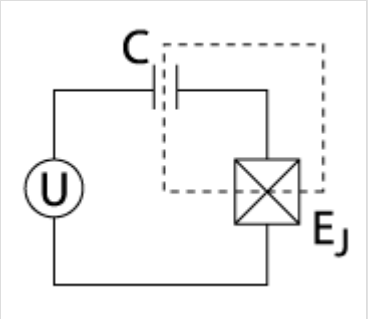
- IBM Quantum (https://www.ibm.com/quantum-computing/systems/) offers access to over 20 quantum computer systems.
- The IBM Quantum Experience (http://www.research.ibm.com/quantum/) offers free access to writing quantum algorithms and executing them on 5 qubit quantum computers.
- IBM's roadmap for quantum computing (https://research.ibm.com/blog/quantum-development-roadmap/) shows 65 qubit systems available in 2020 and 127 qubits to be available sometime in 2021.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Superconducting_quantum_computing&oldid=1242253064"

WIKIPEDIA
The Free Encyclopedia

Charge qubit

In quantum computing, a **charge qubit** (also known as **Cooper-pair box**) is a qubit whose basis states are charge states (i.e. states which represent the presence or absence of excess Cooper pairs in the island).[1][2][3] In superconducting quantum computing, a charge qubit[4] is formed by a tiny superconducting island coupled by a Josephson junction (or practically, superconducting tunnel junction) to a superconducting reservoir (see figure). The state of the qubit is determined by the number of Cooper pairs that have tunneled across the junction. In contrast with the charge state of an atomic or molecular ion, the charge states of such an "island" involve a macroscopic number of conduction electrons of the island. The quantum superposition of charge states can be achieved by tuning the gate voltage U that controls the chemical potential of the island. The charge qubit is typically read-out by electrostatically coupling the island to an extremely sensitive electrometer such as the radio-frequency single-electron transistor.



Circuit diagram of a charge qubit circuit. The island (dotted line) is formed by the superconducting electrode between the gate capacitor and the junction capacitance.

Typical T_2 coherence times for a charge qubit are on the order of 1–2 μs.[5] Recent work has shown T_2 times approaching 100 μs using a type of charge qubit known as a transmon inside a three-dimensional superconducting cavity.[6][7] Understanding the limits of T_2 is an active area of research in the field of superconducting quantum computing.

Fabrication

Charge qubits are fabricated using techniques similar to those used for microelectronics. The devices are usually made on silicon or sapphire wafers using electron beam lithography (different from phase qubit, which uses photolithography) and metallic thin film evaporation processes. To create Josephson junctions, a technique known as shadow evaporation is normally used; this involves evaporating the source metal alternately at two angles through the lithography defined mask in the electron beam resist. This results in two overlapping layers of the superconducting metal, in between which a thin layer of insulator (normally aluminum oxide) is deposited.

Hamiltonian

If the Josephson junction has a junction capacitance C_J, and the gate capacitor C_g, then the charging (Coulomb) energy of one Cooper pair is:

$$E_\mathrm{C} = (2e)^2/2(C_\mathrm{g} + C_\mathrm{J}).$$

If n denotes the number of excess Cooper pairs in the island (i.e. its net charge is $-2ne$), then the Hamiltonian is:[4]

$$H = \sum_n \left[E_\mathrm{C}(n - n_\mathrm{g})^2 |n\rangle\langle n| - \frac{1}{2}E_\mathrm{J}(|n\rangle\langle n+1| + |n+1\rangle\langle n|)\right],$$

where $n_\mathrm{g} = C_\mathrm{g}V_\mathrm{g}/(2e)$ is a control parameter known as effective offset charge (V_g is the gate voltage), and E_J the Josephson energy of the tunneling junction.

At low temperature and low gate voltage, one can limit the analysis to only the lowest $n = 0$ and $n = 1$ states, and therefore obtain a two-level quantum system (a.k.a. qubit).

Note that some recent papers[8][9] adopt a different notation, and define the charging energy as that of one electron:

$$E_\mathrm{C} = e^2/2(C_\mathrm{g} + C_\mathrm{J}),$$

and then the corresponding Hamiltonian is:

$$H = \sum_n \left[4E_\mathrm{C}(n - n_\mathrm{g})^2 |n\rangle\langle n| - \frac{1}{2}E_\mathrm{J}(|n\rangle\langle n+1| + |n+1\rangle\langle n|)\right].$$

Benefits

To-date, the realizations of qubits that have had the most success are ion traps and NMR, with Shor's algorithm even being implemented using NMR.[10] However, it is hard to see these two methods being scaled to the hundreds, thousands, or millions of qubits necessary to create a quantum computer. Solid-state representations of qubits are much more easily scalable, but they themselves have their own problem: decoherence. Superconductors, however, have the advantage of being more easily scaled, and they are more coherent than normal solid-state systems.[10]

Experimental progresses

The implementation of Superconducting charge qubits have been progressing quickly since 1996. Design was theoretically described in 1997 by Shnirman,[11] while the evidence of quantum coherence of the charge in a Cooper pair box was published in February 1997 by Vincent Bouchiat et al.[12] In 1999, coherent oscillations in the charge Qubit were first observed by Nakamura et al.[13] Manipulation of the quantum states and full realization of the charge qubit was observed 2 years later.[14] In 2007, a more advanced device known as Transmon showing enhanced coherence times due to its reduced sensitivity to charge noise was developed at Yale University by Robert J. Schoelkopf, Michel Devoret, Steven M. Girvin and their colleagues .

References

1. Bouchiat, V.; Vion, D.; Joyez, P.; Esteve, D.; Devoret, M. H. (1998). "Quantum Coherence with a Single Cooper Pair". *Physica Scripta*. **T76** (1). IOP Publishing: 165-170. Bibcode:1998PhST...76..165B (https://ui.adsabs.harvard.edu/abs/1998PhST...76..165B). doi:10.1238/physica.topical.076a00165 (https://doi.org/10.1238%2Fphysica.topical.076a001

65). ISSN 0031-8949 (https://search.worldcat.org/issn/0031-8949). S2CID 250887469 (https://api.semanticscholar.org/CorpusID:250887469).

2. Nakamura, Y.; Pashkin, Yu. A.; Tsai, J. S. (1999). "Coherent control of macroscopic quantum states in a single-Cooper-pair box". *Nature*. **398** (6730). Springer Science and Business Media LLC: 786–788. arXiv:cond-mat/9904003 (https://arxiv.org/abs/cond-mat/9904003). Bibcode:1999Natur.398..786N (https://ui.adsabs.harvard.edu/abs/1999Natur.398..786N). doi:10.1038/19718 (https://doi.org/10.1038%2F19718). ISSN 0028-0836 (https://search.worldcat.org/issn/0028-0836). S2CID 4392755 (https://api.semanticscholar.org/CorpusID:4392755).
3. Lehnert, K. W.; Bladh, K.; Spietz, L. F.; Gunnarsson, D.; Schuster, D. I.; et al. (2003-01-17). "Measurement of the Excited-State Lifetime of a Microelectronic Circuit". *Physical Review Letters*. **90** (2). American Physical Society (APS): 027002. Bibcode:2003PhRvL..90b7002L (https://ui.adsabs.harvard.edu/abs/2003PhRvL..90b7002L). doi:10.1103/physrevlett.90.027002 (https://doi.org/10.1103%2Fphysrevlett.90.027002). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 12570573 (https://pubmed.ncbi.nlm.nih.gov/12570573).
4. Makhlin, Yuriy; Schoen, Gerd; Shnirman, Alexander (2001-05-08). "Quantum state engineering with Josephson-junction devices". *Reviews of Modern Physics*. **73** (2): 357–400. arXiv:cond-mat/0011269 (https://arxiv.org/abs/cond-mat/0011269). Bibcode:2001RvMP...73..357M (https://ui.adsabs.harvard.edu/abs/2001RvMP...73..357M). doi:10.1103/RevModPhys.73.357 (https://doi.org/10.1103%2FRevModPhys.73.357). ISSN 0034-6861 (https://search.worldcat.org/issn/0034-6861). S2CID 6687697 (https://api.semanticscholar.org/CorpusID:6687697).
5. Houck, A. A.; Koch, Jens; Devoret, M. H.; Girvin, S. M.; Schoelkopf, R. J. (2009-02-11). "Life after charge noise: recent results with transmon qubits". *Quantum Information Processing*. **8** (2–3): 105–115. arXiv:0812.1865 (https://arxiv.org/abs/0812.1865). doi:10.1007/s11128-009-0100-6 (https://doi.org/10.1007%2Fs11128-009-0100-6). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 27305073 (https://api.semanticscholar.org/CorpusID:27305073).
6. Paik, Hanhee; Schuster, D. I.; Bishop, Lev S.; Kirchmair, G.; Catelani, G.; Sears, A. P.; Johnson, B. R.; Reagor, M. J.; Frunzio, L.; Glazman, L. I.; Girvin, S. M.; Devoret, M. H.; Schoelkopf, R. J. (2011-12-05). "Observation of High Coherence in Josephson Junction Qubits Measured in a Three-Dimensional Circuit QED Architecture". *Physical Review Letters*. **107** (24): 240501. arXiv:1105.4652 (https://arxiv.org/abs/1105.4652). Bibcode:2011PhRvL.107x0501P (https://ui.adsabs.harvard.edu/abs/2011PhRvL.107x0501P). doi:10.1103/physrevlett.107.240501 (https://doi.org/10.1103%2Fphysrevlett.107.240501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 22242979 (https://pubmed.ncbi.nlm.nih.gov/22242979). S2CID 19296685 (https://api.semanticscholar.org/CorpusID:19296685).
7. C. Rigetti *et al.*, "Superconducting qubit in waveguide cavity with coherence time approaching 0.1 ms," arXiv:1202.5533 (https://arxiv.org/abs/1202.5533) (2012)
8. Didier, Nicolas; Sete, Eyob A.; da Silva, Marcus P.; Rigetti, Chad (2018-02-23). "Analytical modeling of parametrically-modulated transmon qubits". *Physical Review A*. **97** (2): 022330. arXiv:1706.06566 (https://arxiv.org/abs/1706.06566). Bibcode:2018PhRvA..97b2330D (https://ui.adsabs.harvard.edu/abs/2018PhRvA..97b2330D). doi:10.1103/PhysRevA.97.022330 (https://doi.org/10.1103%2FPhysRevA.97.022330). ISSN 2469-9926 (https://search.worldcat.org/issn/2469-9926). S2CID 118921729 (https://api.semanticscholar.org/CorpusID:118921729).

9. Schreier, J. A.; Houck, A. A.; Koch, Jens; Schuster, D. I.; Johnson, B. R.; Chow, J. M.; Gambetta, J. M.; Majer, J.; Frunzio, L.; Devoret, M. H.; Girvin, S. M. (2008-05-12). "Suppressing Charge Noise Decoherence in Superconducting Charge Qubits". *Physical Review B*. **77** (18): 180502. arXiv:0712.3581 (https://arxiv.org/abs/0712.3581). Bibcode:2008PhRvB..77r0502S (https://ui.adsabs.harvard.edu/abs/2008PhRvB..77r0502S). doi:10.1103/PhysRevB.77.180502 (https://doi.org/10.1103%2FPhysRevB.77.180502). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 119181860 (https://api.semanticscholar.org/CorpusID:119181860).
10. Superconducting Charge Qubits (http://www.bristol.ac.uk/physics/media/theory-theses/rodrigues-da-thesis.pdf), by Denzil Anthony Rodrigues, page 3
11. Shnirman, Alexander; Schön, Gerd; Hermon, Ziv (22 September 1997). "Quantum Manipulations of Small Josephson Junctions". *Physical Review Letters*. **79** (12): 2371–2374. arXiv:cond-mat/9706016 (https://arxiv.org/abs/cond-mat/9706016). Bibcode:1997PhRvL..79.2371S (https://ui.adsabs.harvard.edu/abs/1997PhRvL..79.2371S). doi:10.1103/physrevlett.79.2371 (https://doi.org/10.1103%2Fphysrevlett.79.2371). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). S2CID 15467259 (https://api.semanticscholar.org/CorpusID:15467259).
12. Vincent Bouchiat (21 February 1997). *Quantum Coherence of the Charge in a single-Cooper-pair box circuit* (https://iramis.cea.fr/drecam/spec/Pres/Quantro/Qsite/publi/theses/VBouchiatThesis.pdf) (PDF) (PhD). Paris 6 University.
13. Nakamura, Yasunobu; Pashkin, Yu; Tsai, JS (29 April 1999). "Coherent control of macroscopic quantum states in a single-Cooper-pair box". *Nature*. **398** (6730): 786–788. arXiv:cond-mat/9904003 (https://arxiv.org/abs/cond-mat/9904003). Bibcode:1999Natur.398..786N (https://ui.adsabs.harvard.edu/abs/1999Natur.398..786N). doi:10.1038/19718 (https://doi.org/10.1038%2F19718). S2CID 4392755 (https://api.semanticscholar.org/CorpusID:4392755).
14. Vion, Denis; Aassime, A; Cottet, A; Joyez, Ph; Pothier, H; Urbina, Ch; Esteve, D; Devoret, M (3 May 2002). "Manipulating the quantum state of an electrical circuit". *Science*. **296** (5569): 886–889. arXiv:cond-mat/0205343 (https://arxiv.org/abs/cond-mat/0205343). Bibcode:2002Sci...296..886V (https://ui.adsabs.harvard.edu/abs/2002Sci...296..886V). doi:10.1126/science.1069372 (https://doi.org/10.1126%2Fscience.1069372). PMID 11988568 (https://pubmed.ncbi.nlm.nih.gov/11988568). S2CID 43515935 (https://api.semanticscholar.org/CorpusID:43515935).

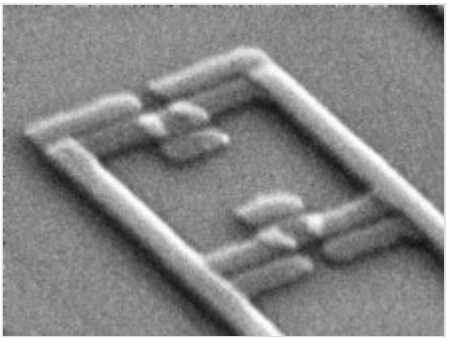
Retrieved from "https://en.wikipedia.org/w/index.php?title=Charge_qubit&oldid=1225952327"

WIKIPEDIA
The Free Encyclopedia

Flux qubit

In quantum computing, more specifically in superconducting quantum computing, **flux qubits** (also known as **persistent current qubits**) are micrometer sized loops of superconducting metal that is interrupted by a number of Josephson junctions. These devices function as quantum bits. The flux qubit was first proposed by Terry P. Orlando et al. at MIT in 1999 and fabricated shortly thereafter.[1] During fabrication, the Josephson junction parameters are engineered so that a persistent current will flow continuously when an external magnetic flux is applied. Only an integer number of flux quanta are allowed to penetrate the superconducting ring, resulting in clockwise or counter-clockwise mesoscopic supercurrents (typically 300 nA[2]) in the loop to compensate (screen or enhance) a non-integer external flux bias. When the applied flux through the loop area is close to a half integer number of flux quanta, the two lowest energy eigenstates of the loop will be a quantum superposition of the clockwise and counter-clockwise currents. The two lowest energy eigenstates differ only by the relative quantum phase between the composing current-direction states. Higher energy eigenstates correspond to much larger (macroscopic) persistent currents, that induce an additional flux quantum to the qubit loop, thus are well separated energetically from the lowest two eigenstates. This separation, known as the "qubit non linearity" criteria, allows operations with the two lowest eigenstates only, effectively creating a two level system. Usually, the two lowest eigenstates will serve as the computational basis for the logical qubit.

Computational operations are performed by pulsing the qubit with microwave frequency radiation which has an energy comparable to that of the gap between the energy of the two basis states, similar to RF-SQUID. Properly selected pulse duration and strength can put the qubit into a quantum superposition of the two basis states while subsequent pulses can manipulate the probability weighting that the qubit will be measured in either of the two basis states, thus performing a computational operation.



SEM image of a 4-junction flux qubit fabricated at Royal Holloway University of London

Fabrication

Flux qubits are fabricated using techniques similar to those used for microelectronics. The devices are usually made on silicon or sapphire wafers using electron beam lithography and metallic thin film evaporation processes. To create Josephson junctions, a technique known as shadow evaporation is normally used; this involves evaporating the source metal alternately at two angles through the lithography defined mask in the electron beam resist. This results in two overlapping layers of the superconducting metal, in between which a thin layer of insulator (normally aluminum oxide) is deposited.[3]

Dr. Shcherbakova's group reported using niobium as the contacts for their flux qubits. Niobium is often used as the contact and is deposited by employing a sputtering technique and using optical lithography to pattern the contacts. An argon beam can then be used to reduce the oxide layer that forms on top of the contacts. The sample must be cooled during the etching process in order to keep the niobium contacts from melting. At this point, the aluminum layers can be deposited on top of the clean niobium surfaces.

The aluminum is then deposited in two steps from alternating angles on the niobium contacts. An oxide layer forms between the two aluminum layers in order to create the $Al/AlO_x/Al$ Josephson junction.[3] In standard flux qubits, 3 or 4 Josephson junctions will be patterned around the loop.

Resonators can be fabricated to measure the readout of the flux qubit through a similar techniques. The resonator can be fabricated by e-beam lithography and CF_4 reactive ion etching of thin films of niobium or a similar metal. The resonator could then be coupled to the flux qubit by fabricating the flux qubit at the end of the resonator.[4]

Flux Qubit Parameters

The flux qubit is distinguished from other known types of superconducting qubit such as the charge qubit or phase qubit by the coupling energy and charging energy of its junctions. In the charge qubit regime the charging energy of the junctions dominates the coupling energy. In a Flux qubit the situation is reversed and the coupling energy dominates. Typically for a flux qubit the coupling energy is 10-100 times greater than the charging energy which allows the Cooper pairs to flow continuously around the loop, rather than tunnel discretely across the junctions like a charge qubit.

Josephson Junctions

In order for a superconducting circuit to function as a qubit, there needs to be a non-linear element. If the circuit has a harmonic oscillator, such as in an LC-circuit, the energy levels are degenerate. This prohibits the formation of a two qubit computational space because any microwave radiation that is applied to manipulate the ground state and the first excited state to perform qubit operations would also excite the higher energy states. Josephson junctions are the only electronic element that are non-linear as well as non-dissipative at low temperatures . These are requirements for quantum integrated circuits, making the Josephson junction essential in the construction of flux qubits.[5] Understanding the physics of the Josephson junction will improve comprehension of how flux qubits operate.

Essentially, Josephson junctions consist of two pieces of superconducting thin film that are separated by a layer of insulator. In the case of flux qubits, Josephson junctions are fabricated by the process that is described above. The wave functions of the superconducting components overlap, and this construction allows for the tunneling of electrons which creates a phase difference between the wave functions on either side of the insulating barrier.[5] This phase difference that is equivalent to $\phi = \phi_2 - \phi_1$, where ϕ_1, ϕ_2 correspond to the wave functions on either side of the tunneling barrier. For this phase difference, the following Josephson relations have been established:

$I_J = I_0 \sin\phi$ [6]

$V = \frac{\Phi_0}{2\pi}\frac{d\phi}{dt}$ [6]

Here, I_J is the Josephson current and Φ_0 is the flux quantum. By differentiating the current equation and using substitution, one obtains the Josephson inductance term L_J:

$$L_J = \frac{\Phi_0}{2\pi I_0 \cos\phi}$$ [6]

From these equations, it can be seen that the Josephson inductance term is non-linear from the cosine term in the denominator; because of this, the energy level spacings are no longer degenerate, restricting the dynamics of the system to the two qubit states. Because of the non-linearity of the Josephson junction, operations using microwaves can be performed on the two lowest energy eigenvalue states (the two qubit states) without exciting the higher energy states. This was previously referred to as the "qubit non linearity" criteria. Thus, Josephson junctions are an integral element of flux qubits and superconducting circuits in general.

Coupling

Coupling between two or more qubits is essential to implement many-qubit gates. The two basic coupling mechanisms are the direct inductive coupling and coupling via a microwave resonator. In the direct coupling, the circulating currents of the qubits inductively affect one another - clockwise current in one qubit induces counter-clockwise current in the other. In the Pauli Matrices formalism, a $\sigma_z\sigma_z$ term appears in the Hamiltonian, essential for the controlled NOT gate implementation.[7] The direct coupling might be further enhanced by kinetic inductance, if the qubit loops are made to share an edge, so that the currents will flow through the same superconducting line. Inserting a Josephson junction on that joint line will add a Josephson inductance term, and increase the coupling even more. To implement a switchable coupling in the direct coupling mechanism, as required to implement a gate of finite duration, an intermediate coupling loop may be used. The control magnetic flux applied to the coupler loop switches the coupling on and off, as implemented, for example, in the D-Wave Systems machines. The second method of coupling uses an intermediate microwave cavity resonator, commonly implemented in a coplanar waveguide geometry. By tuning the energy separation of the qubits to match the one of the resonator, the phases of the loop currents are synchronized, and a $\sigma_x\sigma_x$ coupling is implemented. Tuning the qubits in and out of resonance (for example, by modifying their bias magnetic flux) controls the duration of the gate operation.

Readout

Like all quantum bits, flux qubits require a suitably sensitive probe coupled to it in order to measure its state after a computation has been carried out. Such quantum probes should introduce as little back-action as possible onto the qubit during measurement. Ideally they should be decoupled during computation and then turned "on" for a short time during read-out. Read-out probes for flux qubits work by interacting with one of the qubit's macroscopic variables, such as the circulating current, the flux within the loop or the macroscopic phase of the superconductor. This interaction then changes some variable of the read-out probe which can be measured using conventional low-noise electronics. The read-out probe is typically the technology aspect that separates the research of different University groups working on flux qubits.

Prof. Mooij's group at Delft in the Netherlands,[2] along with collaborators, has pioneered flux qubit technology, and were the first to conceive, propose and implement flux qubits as they are known today. The Delft read-out scheme is based on a SQUID loop that is inductively coupled to the qubit, the qubit's

state influences the critical current of the SQUID. The critical current can then be read-out using ramped measurement currents through the SQUID. Recently the group has used the plasma frequency of the SQUID as the read-out variable.

Dr. Il'ichev's group at IPHT Jena in Germany[8] are using impedance measurement techniques based on the flux qubit influencing the resonant properties of a high quality tank circuit, which, like the Delft group is also inductively coupled to the qubit. In this scheme the qubit's magnetic susceptibility, which is defined by its state, changes the phase angle between the current and voltage when a small A.C. signal is passed into the tank circuit.

Prof. Petrashov's group at Royal Holloway[9] are using an Andreev interferometer probe to read out flux qubits.[10][11] This read-out uses the phase influence of a superconductor on the conductance properties of a normal metal. A length of normal metal is connected at either end to either side of the qubit using superconducting leads, the phase across the qubit, which is defined by its state, is translated into the normal metal, the resistance of which is then read-out using low noise resistance measurements.

Dr. Jerger's group uses resonators that are coupled with the flux qubit. Each resonator is dedicated to just one qubit, and all resonators can be measured with a single transmission line. The state of the flux qubit alters the resonant frequency of the resonator due to a dispersive shift that is picked up by the resonator from the coupling with the flux qubit. The resonant frequency is then measured by the transmission line for each resonator in the circuit. The state of the flux qubit is then determined by the measured shift in the resonant frequency.[4]

References

1. Orlando, T. P.; Mooij, J. E.; Tian, Lin; Van Der Wal, Caspar H.; Levitov, L. S.; Lloyd, Seth; Mazo, J. J. (1999). "Superconducting persistent-current qubit". *Physical Review B*. **60** (22): 15398–15413. arXiv:cond-mat/9908283 (https://arxiv.org/abs/cond-mat/9908283). Bibcode:1999PhRvB..6015398O (https://ui.adsabs.harvard.edu/abs/1999PhRvB..6015398O). doi:10.1103/PhysRevB.60.15398 (https://doi.org/10.1103%2FPhysRevB.60.15398). S2CID 16093985 (https://api.semanticscholar.org/CorpusID:16093985).
2. University of Delft - Flux Qubit Website (http://qt.tn.tudelft.nl/research/fluxqubit/) Archived (https://archive.today/20080301104624/http://qt.tn.tudelft.nl/research/fluxqubit/) 2008-03-01 at archive.today
3. Shcherbakova, A V (13 January 2015). "Fabrication and measurements of hybrid Nb/Al Josephson junctions and flux qubits with π-shifters" (https://iopscience.iop.org/article/10.1088/0953-2048/28/2/025009/meta). *Superconductor Science and Technology*. **28** (2): 025009. arXiv:1405.0373 (https://arxiv.org/abs/1405.0373). Bibcode:2015SuScT..28b5009S (https://ui.adsabs.harvard.edu/abs/2015SuScT..28b5009S). doi:10.1088/0953-2048/28/2/025009 (https://doi.org/10.1088%2F0953-2048%2F28%2F2%2F025009). S2CID 118577242 (https://api.semanticscholar.org/CorpusID:118577242).
4. Jerger, M.; Poletto, S.; Macha, P.; Hübner, U.; Lukashenko, A.; Il\textquotesingleichev, E.; Ustinov, A. V. (November 2011). "Readout of a qubit array via a single transmission line" (https://doi.org/10.1209%2F0295-5075%2F96%2F40012). *EPL (Europhysics Letters)*. **96** (4): 40012. arXiv:1102.0404 (https://arxiv.org/abs/1102.0404). Bibcode:2011EL.....9640012J (https://ui.adsabs.harvard.edu/abs/2011EL.....9640012J). doi:10.1209/0295-5075/96/40012 (https://doi.org/10.1209%2F0295-5075%2F96%2F40012). ISSN 0295-5075 (https://search.worldcat.org/issn/0295-5075). S2CID 59796640 (https://api.semanticscholar.org/CorpusID:59796640).

5. Devoret, M. & Wallraff, Andreas & Martinis, J.M.. (2004). Superconducting Qubits: A Short Review.
6. Martinis, John & Osborne, Kevin. Superconducting Qubits and the Physics of Josephson Junctins. Les Houches, 2004.
7. Nielsen, Michael A.; Chuang, Isaac L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press. ISBN 0-521-63235-8.
8. University of Jena - Flux Qubit Website (http://www.ipht-jena.de/BEREICH_1/abt13_cryo_electronics/application-data/computing.php) Archived (https://web.archive.org/web/20070214111933/http://www.ipht-jena.de/BEREICH_1/abt13_cryo_electronics/application-data/computing.php) February 14, 2007, at the Wayback Machine
9. Royal Holloway University of London - Flux Qubit Website (http://www.rhul.ac.uk/physics/research/postgraduateopportunities/nanophysicsnanotechnology/superconductorfluxqubits.aspx)
10. Checkley, C.; Iagallo, A.; Shaikhaidarov, R.; Nicholls, J. T.; Petrashov, V. T. (2011-04-06). "Andreev Interferometers in a Strong Radio Frequency Field". *Journal of Physics: Condensed Matter*. **23** (13): 135301. arXiv:1003.2785 (https://arxiv.org/abs/1003.2785). Bibcode:2011JPCM...23m5301C (https://ui.adsabs.harvard.edu/abs/2011JPCM...23m5301C). doi:10.1088/0953-8984/23/13/135301 (https://doi.org/10.1088%2F0953-8984%2F23%2F13%2F135301). ISSN 0953-8984 (https://search.worldcat.org/issn/0953-8984). PMID 21403240 (https://pubmed.ncbi.nlm.nih.gov/21403240). S2CID 24551976 (https://api.semanticscholar.org/CorpusID:24551976).
11. Petrashov, V. T.; Chua, K. G.; Marshall, K. M.; Shaikhaidarov, R. Sh; Nicholls, J. T. (2005-09-27). "Andreev Probe of Persistent Current States in Superconducting Quantum Circuits". *Physical Review Letters*. **95** (14): 147001. arXiv:cond-mat/0503061 (https://arxiv.org/abs/cond-mat/0503061). Bibcode:2005PhRvL..95n7001P (https://ui.adsabs.harvard.edu/abs/2005PhRvL..95n7001P). doi:10.1103/PhysRevLett.95.147001 (https://doi.org/10.1103%2FPhysRevLett.95.147001). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 16241686 (https://pubmed.ncbi.nlm.nih.gov/16241686). S2CID 963004 (https://api.semanticscholar.org/CorpusID:963004).

- Devoret, Michel H.; Martinis, John M. (2005). "Implementing qubits with superconducting integrated circuits". *Experimental Aspects of Quantum Computing*: 163–203. doi:10.1007/0-387-27732-3_12 (https://doi.org/10.1007%2F0-387-27732-3_12). ISBN 978-0-387-23045-0.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Flux_qubit&oldid=1191808071"

WIKIPEDIA
The Free Encyclopedia

Phase qubit

In quantum computing, and more specifically in superconducting quantum computing, the **phase qubit** is a superconducting device based on the superconductor–insulator–superconductor (SIS) Josephson junction,[1] designed to operate as a quantum bit, or qubit.[2]

The phase qubit is closely related, yet distinct from, the flux qubit and the charge qubit, which are also quantum bits implemented by superconducting devices. The major distinction among the three is the ratio of Josephson energy vs charging energy[3] (the necessary energy for one Cooper pair to *charge* the total capacitance in the circuit):

- For phase qubit, this ratio is on the order of 10^6, which allows for macroscopic bias current through the junction;
- For flux qubit it's on the order of 10, which allows for mesoscopic supercurrents (typically ~300 nA[4]);
- For charge qubit it's less than 1, and therefore only a few Cooper pairs can tunnel through and charge the Cooper-pair box. However, transmon can have a very low charging energy due to the huge shunt capacitance, and therefore have this ratio on the order of 10~100.[5]

Introduction

A phase qubit is a current-biased Josephson junction, operated in the zero voltage state with a non-zero current bias.

A Josephson junction is a tunnel junction,[6] made of two pieces of superconducting metal separated by a very thin insulating barrier, about 1 nm in thickness. The barrier is thin enough that electrons, or in the superconducting state, Cooper-paired electrons, can tunnel through the barrier at an appreciable rate. Each of the superconductors that make up the Josephson junction is described by a macroscopic wavefunction, as described by the Ginzburg–Landau theory for superconductors.[7] The difference in the complex phases of the two superconducting wavefunctions is the most important dynamic variable for the Josephson junction, and is called the phase difference δ, or simply "phase".

Main equations describing the SIS junction

The Josephson equation[1] relates the superconducting current (usually called the supercurrent) I through the tunnel junction to the phase difference δ,

$$I = I_0 \sin\delta \text{ (Josephson current-phase relationship)}$$

Here I_0 is the critical current of the tunnel junction, determined by the area and thickness of the tunnel barrier in the junction, and by the properties of the superconductors on either side of the barrier. For a junction with identical superconductors on either side of the barrier, the critical current is related to the superconducting gap Δ and the normal state resistance R_n of the tunnel junction by the Ambegaokar–Baratoff formula [6]

$$I_0 = \frac{\pi\Delta}{2eR_n}$$ (Ambegaokar–Baratoff formula)

The Gor'kov phase evolution equation[1] gives the rate of change of the phase (the "velocity" of the phase) as a linear function of the voltage V as

$$V = \frac{\hbar}{2e}\frac{d\delta}{dt}$$ (Gor'kov-Josephson phase evolution equation)

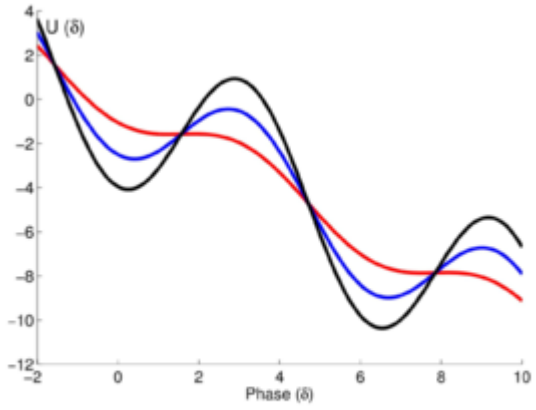
This equation is a generalization of the Schrödinger equation for the phase of the BCS wavefunction. The generalization was carried out by Gor'kov in 1958.[8]

The McCumber–Stewart model

The alternative and direct current Josephson relations control the behavior of the Josephson junction itself. The geometry of the Josephson junction—two plates of superconducting metal separated by a thin tunnel barrier—is that of a parallel plate capacitor, so in addition to the Josephson element the device includes a parallel capacitance C. The external circuit is usually simply modeled as a resistor R in parallel with the Josephson element. The set of three parallel circuit elements is biased by an external current source I, thus the current-biased Josephson junction.[9] Solving the circuit equations yields a single dynamic equation for the phase,

$$\frac{\hbar C}{2e}\frac{d^2\delta}{dt^2} + \frac{\hbar}{2eR}\frac{d\delta}{dt} = I - I_0\sin\delta.$$

The terms on the left side are identical to those of a particle with coordinate (location) δ, with mass proportional to the capacitance C, and with friction inversely proportional to the resistance R. The particle moves in a conservative force field given by the term on the right, which corresponds to the particle interacting with a potential energy $U(\delta)$ given by



$$U(\delta) = \frac{\hbar}{2e}\left(-I_0\cos\delta - I\,\delta\right).$$

This is the "washboard potential",[9] so-called because it has an overall linear dependence $-I\,\delta$, modulated by the washboard modulation $-I_0\,\cos\delta$.

The zero voltage state describes one of the two distinct dynamic behaviors displayed by the phase particle, and corresponds to when the particle is trapped in one of the local minima in the washboard potential. These minima exist for bias currents $|I| < I_0$, i.e. for currents below the critical current. With the phase particle trapped in a minimum, it has zero average velocity and therefore zero average voltage. A Josephson junction will allow currents up to I_0 to pass through without any voltage; this corresponds to the superconducting branch of the Josephson junction's current–voltage characteristic.

The voltage state is the other dynamic behavior displayed by a Josephson junction, and corresponds to the phase particle free-running down the slope of the potential, with a non-zero average velocity and therefore non-zero voltage. This behavior always occurs for currents I above the critical current, i.e. for $|I| > I_0$, and for large resistances R also occurs for currents somewhat below the critical current. This state corresponds to the voltage branch of the Josephson junction current–voltage characteristic. For large resistance junctions the zero-voltage and voltage branches overlap for some range of currents below the critical current, so the device behavior is hysteretic.

Nonlinear inductor

Another way to understand the behavior of a Josephson junction in the zero-voltage state is to consider the SIS tunnel junction as a nonlinear inductor.[10] When the phase is trapped in one of the minima, the phase value is limited to a small range about the phase value at the potential minimum, which we will call δ_0. The current through the junction is related to this phase value by

$$I = I_0 \sin \delta_0.$$

If we consider small variations $\Delta\delta$ in the phase about the minimum δ_0 (small enough to maintain the junction in the zero voltage state), then the current will vary by

$$\Delta I = (I_0 \cos \delta_0)\, \Delta\delta.$$

These variations in the phase give rise to a voltage through the ac Josephson relation,

$$\Delta V = \frac{\hbar}{2e} \frac{d\Delta\delta}{dt} = \frac{\hbar}{2e} \frac{1}{I_0 \cos \delta_0} \frac{d\Delta I}{dt} = L \frac{d\Delta I}{dt}$$

This last relation is the defining equation for an inductor with inductance

$$L = \frac{\hbar}{2e} \frac{1}{I_0 \cos \delta_0}.$$

This inductance depends on the value of phase δ_0 at the minimum in the washboard potential, so the inductance value can be controlled by changing the bias current I. For zero bias current, the inductance reaches its minimum value,

$$L_{\min} = \frac{\hbar}{2e} \frac{1}{I_0} = \frac{\hbar R_n}{\pi \Delta}.$$

As the bias current increases, the inductance increases. When the bias current is very close (but less than) the critical current I_0, the value of the phase δ_0 is very close to $\pi/2$, as seen by the dc Josephson relation, above. This means that the inductance value L becomes very large, diverging as I reaches the critical current I_0.

The nonlinear inductor represents the response of the Josephson junction to changes in bias current. When the parallel capacitance from the device geometry is included, in parallel with the inductor, this forms a nonlinear LC resonator, with resonance frequency

$$\omega_p = \frac{1}{\sqrt{LC}} = \sqrt{\frac{2eI_0 \cos\delta_0}{\hbar C}},$$

which is known as the plasma frequency of the junction. This corresponds to the oscillation frequency of the phase particle in the bottom of one of the minima of the washboard potential.

For bias currents very near the critical current, the phase value in the washboard minimum is

$$\cos\delta_0 = \sqrt{1-(I/I_0)^2},$$

and the plasma frequency is then

$$\omega_p \approx \sqrt{\frac{2eI_0}{\hbar C}}\left[1-(I/I_0)^2\right]^{1/4},$$

clearly showing that the plasma frequency approaches zero as the bias current approaches the critical current.

The simple tunability of the current-biased Josephson junction in its zero voltage state is one of the key advantages the phase qubit has over some other qubit implementations, although it also limits the performance of this device, as fluctuations in current generate fluctuations in the plasma frequency, which causes dephasing of the quantum states.

Quantized energy levels

The phase qubit is operated in the zero-voltage state, with $|I| < I_0$. At very low temperatures, much less than 1 K (achievable using a cryogenic system known as a dilution refrigerator), with a sufficiently high resistance and small capacitance Josephson junction, quantum energy levels [11] become detectable in the local minima of the washboard potential. These were first detected using microwave spectroscopy, where a weak microwave signal is added to the current I biasing the junction. Transitions from the zero voltage state to the voltage state were measured by monitoring the voltage across the junction. Clear resonances at certain frequencies were observed, which corresponded well with the quantum transition energies obtained by solving the Schrödinger equation[12] for the local minimum in the washboard potential. Classically only a single resonance is expected, centered at the plasma frequency ω_p. Quantum mechanically, the potential minimum in the washboard potential can accommodate several quantized energy levels, with the lowest (ground to first excited state) transition at an energy $E_{01} \approx \hbar\omega_p$, but the higher energy transitions (first to second excited state, second to third excited state) shifted somewhat below this due to the non-harmonic nature of the trapping potential minimum, whose resonance frequency falls as the energy increases in the minimum. Observing multiple, discrete levels in this fashion is extremely strong evidence that the superconducting device is behaving quantum mechanically, rather than classically.

The phase qubit uses the lowest two energy levels in the local minimum; the ground state $|g\rangle$ is the "zero state" of the qubit, and the first excited state $|e\rangle$ is the "one state". The slope in the washboard potential is set by the bias current I, and changes in this current change the washboard potential, changing the shape

of the local minimum (equivalently, changing the value of the nonlinear inductance, as discussed above). This changes the energy difference between the ground and first excited states. Hence the phase qubit has a tunable energy splitting.

References

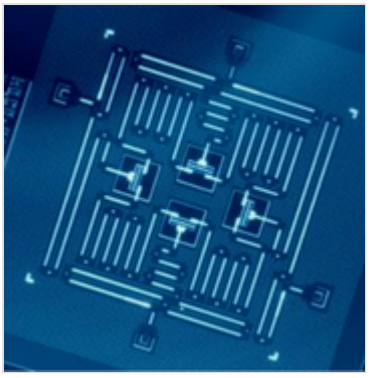
1. Barone, Antonio; Paterno, Gianfranco (1981). *Physics and Applications of the Josephson Effect*. New York: Wiley.
2. Nielsen, Michael; Chuang, Isaac (2000). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.
3. You, J. Q.; Nori, Franco (2007-01-12). "Superconducting Circuits and Quantum Information" (https://physicstoday.scitation.org/doi/abs/10.1063/1.2155757). *Physics Today*. **58** (11): 42. arXiv:quant-ph/0601121 (https://arxiv.org/abs/quant-ph/0601121). doi:10.1063/1.2155757 (https://doi.org/10.1063%2F1.2155757). ISSN 0031-9228 (https://search.worldcat.org/issn/0031-9228). S2CID 10969948 (https://api.semanticscholar.org/CorpusID:10969948).
4. University of Delft - Flux Qubit Website (http://qt.tn.tudelft.nl/research/fluxqubit/) Archived (https://archive.today/20080301104624/http://qt.tn.tudelft.nl/research/fluxqubit/) 2008-03-01 at archive.today
5. Schreier, J. A.; Houck, A. A.; Koch, Jens; Schuster, D. I.; Johnson, B. R.; Chow, J. M.; Gambetta, J. M.; Majer, J.; Frunzio, L.; Devoret, M. H.; Girvin, S. M. (2008-05-12). "Suppressing charge noise decoherence in superconducting charge qubits" (https://link.aps.org/doi/10.1103/PhysRevB.77.180502). *Physical Review B*. **77** (18): 180502. arXiv:0712.3581 (https://arxiv.org/abs/0712.3581). Bibcode:2008PhRvB..77r0502S (https://ui.adsabs.harvard.edu/abs/2008PhRvB..77r0502S). doi:10.1103/PhysRevB.77.180502 (https://doi.org/10.1103%2FPhysRevB.77.180502). S2CID 119181860 (https://api.semanticscholar.org/CorpusID:119181860).
6. van Duzer, Theodore; Turner, Charles (1999). *Principles of Superconductive Devices and Circuits, 2nd ed*. Upper Saddle River NJ: Prentice-Hall.
7. Tinkham, Michael; Paterno, Gianfranco (1996). *Introduction to Superconductivity*. New York: McGraw-Hill.
8. L. P. Gor'kov (1958). "On the energy spectrum of superconductors" (http://jetp.ras.ru/cgi-bin/e/index/e/7/3/p505?a=list). *Sov. Phys. JETP*. **7** (3): 505.
9. Likharev, Konstantin (1986). *Dynamics of Josephson Junctions and Circuits*. New York: Gordon and Breach.
10. Devoret, Michel; Martinis, John (2004). "Superconducting Qubits". In Esteve, Daniel; Raimond, J.-M.; Dalibard, J. (eds.). *Quantum Entanglement and Information Processing*. Elsevier. ISBN 0-444-51728-6.
11. J. M. Martinis; M. Devoret; J. Clarke (1985). "Energy-level quantization in the zero-voltage state of a current-biased Josephson junction" (https://zenodo.org/record/1233847). *Phys. Rev. Lett*. **55** (15): 1543–1546. Bibcode:1985PhRvL..55.1543M (https://ui.adsabs.harvard.edu/abs/1985PhRvL..55.1543M). doi:10.1103/PhysRevLett.55.1543 (https://doi.org/10.1103%2FPhysRevLett.55.1543). PMID 10031852 (https://pubmed.ncbi.nlm.nih.gov/10031852).
12. Griffiths, David J. (2004). *Introduction to Quantum Mechanics, 2nd ed*. New York: Benjamin Cummings. ISBN 0-13-111892-7.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Phase_qubit&oldid=1092351358"

WIKIPEDIA
The Free Encyclopedia

Transmon

In quantum computing, and more specifically in superconducting quantum computing, a **transmon** is a type of superconducting charge qubit designed to have reduced sensitivity to charge noise. The transmon was developed by Robert J. Schoelkopf, Michel Devoret, Steven M. Girvin, and their colleagues at Yale University in 2007.[1][2] Its name is an abbreviation of the term *transmission line shunted plasma oscillation qubit*; one which consists of a Cooper-pair box "where the two superconductors are also [capacitively] shunted in order to decrease the sensitivity to charge noise, while maintaining a sufficient anharmonicity for selective qubit control".[3]



A device consisting of four transmon qubits, four quantum buses, and four readout resonators fabricated by IBM and published in *npj Quantum Information* in January 2017.[4]

The transmon achieves its reduced sensitivity to charge noise by significantly increasing the ratio of the Josephson energy to the charging energy. This is accomplished through the use of a large shunting capacitor. The result is energy level spacings that are approximately independent of offset charge. Planar on-chip transmon qubits have T_1 coherence times approximately 30 μs to 40 μs.[5] Recent work has shown significantly improved T_1 times as long as 95 μs by replacing the superconducting transmission line cavity with a three-dimensional superconducting cavity,[6][7] and by replacing niobium with tantalum in the transmon device, T_1 is further improved up to 0.3 ms.[8] These results demonstrate that previous T_1 times were not limited by Josephson junction losses. Understanding the fundamental limits on the coherence time in superconducting qubits such as the transmon is an active area of research.

Comparison to Cooper-pair box

The transmon design is similar to the first design of the charge qubit[9] known as a "Cooper-pair box"; both are described by the same Hamiltonian, with the only difference being the $E_\mathrm{J}/E_\mathrm{C}$ ratio. Here E_J is the Josephson energy of the junction, and E_C is the charging energy inversely proportional to the total capacitance of the qubit circuit. Transmons typically have $E_\mathrm{J}/E_\mathrm{C} \gg 1$ (while $E_\mathrm{J}/E_\mathrm{C} \lesssim 1$ for typical Cooper-pair-box qubits), which is achieved by shunting the Josephson junction with an additional large capacitor.

The benefit of increasing the $E_\mathrm{J}/E_\mathrm{C}$ ratio is the insensitivity to charge noise—the energy levels become independent of the offset charge n_g across the junction; thus the dephasing time of the qubit is prolonged. The disadvantage is the reduced anharmonicity $\alpha = (E_{21} - E_{10})/E_{10}$, where E_{ij} is the energy difference between eigenstates $|i\rangle$ and $|j\rangle$. Reduced anharmonicity complicates the device operation as a two level system, e.g. exciting the device from the ground state to the first excited state by a resonant pulse also populates the higher excited state. This complication is overcome by complex microwave pulse design, that takes into account the higher energy levels, and prohibits their excitation by destructive interference. Also, while the variation of $E_{10}$with respect to n_g tend to decrease exponentially with

E_J/E_C, the anharmonicity only has a weaker, algebraic dependence on E_J/E_C as $\sim (E_J/E_C)^{-1/2}$. The significant gain in the coherence time outweigh the decrease in the anharmonicity for controlling the states with high fidelity.

Measurement, control and coupling of transmons is performed by means of microwave resonators with techniques from circuit quantum electrodynamics also applicable to other superconducting qubits. Coupling to the resonators is done by placing a capacitor between the qubit and the resonator, at a point where the resonator electromagnetic field is greatest. For example, in IBM Quantum Experience devices, the resonators are implemented with "quarter wave" coplanar waveguides with maximal field at the signal-ground short at the waveguide end; thus every IBM transmon qubit has a long resonator "tail". The initial proposal included similar transmission line resonators coupled to every transmon, becoming a part of the name. However, charge qubits operated at a similar E_J/E_C regime, coupled to different kinds of microwave cavities are referred to as transmons as well.

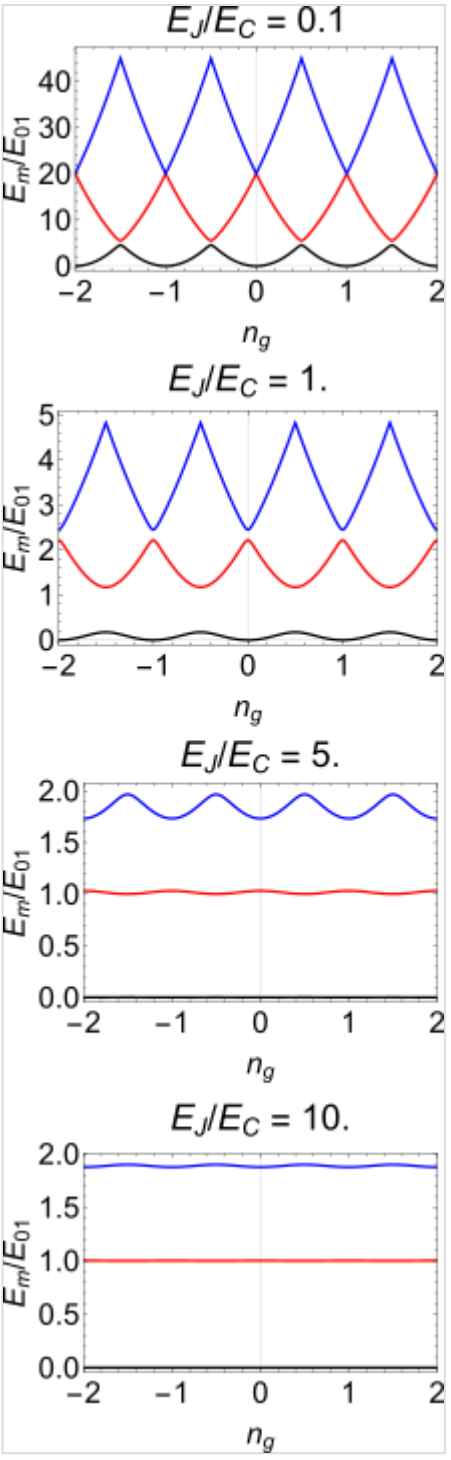
Transmons as qudits

Transmons have been explored for use as *d*-dimensional qudits via the additional energy levels that naturally occur above the qubit subspace (the lowest two states). For example, the lowest *three* levels can be used to make a transmon qutrit; in the early 2020s, researchers have reported realizations of single-qutrit quantum gates on transmons[10][11] as well as two-qutrit entangling gates.[12] Entangling gates on transmons have also been explored theoretically and in simulations for the general case of qudits of arbitrary *d*.[13]

See also

- Charge qubit
- Anharmonicity
- Circuit quantum electrodynamics (cQED)
- Dilution refrigerator
- List of quantum processors
- Quantum harmonic oscillator
- Superconducting quantum computing

References



Eigenenergies E_m (first three levels, $m = 0, 1, 2$) of the qubit Hamiltonian as a function of the effective offset charge n_g for different ratios E_J/E_c. Energies are given in units of the transition energy E_{01}, evaluated at the degeneracy point $n_g = 0.5$. The zero point of energy is chosen as the bottom of the $m = 0$ level. The charge qubit (small E_J/E_c, top) is normally operated at the $n_g = 0.5$ "sweet spot", where fluctuations in cause less energy shift, and the anharmonicity is maximal.

1. Koch, Jens; Yu, Terri M.; Gambetta, Jay; Houck, A. A.; Schuster, D. I.; Majer, J.; Blais, Alexandre; Devoret, M. H.; Girvin, S. M.; Schoelkopf, R. J. (2007-10-12). "Charge-insensitive qubit design derived from the Cooper pair box". *Physical Review A*. **76** (4): 042319. arXiv:cond-mat/0703002 (https://arxiv.org/abs/cond-mat/0703002). Bibcode:2007PhRvA..76d2319K (https://ui.adsabs.harvard.edu/abs/2007PhRvA..76d2319K). doi:10.1103/physreva.76.042319 (https://doi.org/10.1103%2Fphysreva.76.042319). ISSN 1050-2947 (https://search.worldcat.org/issn/1050-2947). S2CID 53983107 (https://api.semanticscholar.org/CorpusID:53983107).
2. Schreier, J. A.; Houck, A. A.; Koch, Jens; Schuster, D. I.; Johnson, B. R.; et al. (2008-05-12). "Suppressing charge noise decoherence in superconducting charge qubits". *Physical Review B*. **77** (18). American Physical Society (APS): 180402. arXiv:0712.3581 (https://arxiv.org/abs/0712.3581). Bibcode:2008PhRvB..77r0502S (https://ui.adsabs.harvard.edu/abs/2008PhRvB..77r0502S). doi:10.1103/physrevb.77.180502 (https://doi.org/10.1103%2Fphysrevb.77.180502). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 119181860 (https://api.semanticscholar.org/CorpusID:119181860).
3. Fink, Johannes M. (2010). *Quantum Nonlinearities in Strong Coupling Circuit QED* (Ph.D.). ETH Zurich.
4. Gambetta, Jay M.; Chow, Jerry M.; Steffen, Matthias (2017-01-13). "Building logical qubits in a superconducting quantum computing system" (https://doi.org/10.1038%2Fs41534-016-0004-0). *npj Quantum Information*. **3** (1). Springer Science and Business Media LLC: 2. arXiv:1510.04375 (https://arxiv.org/abs/1510.04375). Bibcode:2017npjQI...3....2G (https://ui.adsabs.harvard.edu/abs/2017npjQI...3....2G). doi:10.1038/s41534-016-0004-0 (https://doi.org/10.1038%2Fs41534-016-0004-0). ISSN 2056-6387 (https://search.worldcat.org/issn/2056-6387). S2CID 118517248 (https://api.semanticscholar.org/CorpusID:118517248).
5. Barends, R.; Kelly, J.; Megrant, A.; Sank, D.; Jeffrey, E.; et al. (2013-08-22). "Coherent Josephson Qubit Suitable for Scalable Quantum Integrated Circuits". *Physical Review Letters*. **111** (8): 080502. arXiv:1304.2322 (https://arxiv.org/abs/1304.2322). Bibcode:2013PhRvL.111h0502B (https://ui.adsabs.harvard.edu/abs/2013PhRvL.111h0502B). doi:10.1103/physrevlett.111.080502 (https://doi.org/10.1103%2Fphysrevlett.111.080502). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 24010421 (https://pubmed.ncbi.nlm.nih.gov/24010421). S2CID 27081288 (https://api.semanticscholar.org/CorpusID:27081288).

Transmon (large E_J/E_c, bottom) energy levels are insensitive to fluctuations, but the anharmonicity is reduced.

6. Paik, Hanhee; Schuster, D. I.; Bishop, Lev S.; Kirchmair, G.; Catelani, G.; et al. (2011-12-05). "Observation of High Coherence in Josephson Junction Qubits Measured in a Three-Dimensional Circuit QED Architecture". *Physical Review Letters*. **107** (24): 240501. arXiv:1105.4652 (https://arxiv.org/abs/1105.4652). Bibcode:2011PhRvL.107x0501P (https://ui.adsabs.harvard.edu/abs/2011PhRvL.107x0501P). doi:10.1103/physrevlett.107.240501 (https://doi.org/10.1103%2Fphysrevlett.107.240501). ISSN 0031-9007 (https://search.worldcat.org/issn/0031-9007). PMID 22242979 (https://pubmed.ncbi.nlm.nih.gov/22242979). S2CID 19296685 (https://api.semanticscholar.org/CorpusID:19296685).
7. Rigetti, Chad; Gambetta, Jay M.; Poletto, Stefano; Plourde, B. L. T.; Chow, Jerry M.; et al. (2012-09-24). "Superconducting qubit in a waveguide cavity with a coherence time approaching 0.1 ms". *Physical Review B*. **86** (10). American Physical Society (APS): 100506. arXiv:1202.5533 (https://arxiv.org/abs/1202.5533). Bibcode:2012PhRvB..86j0506R (https://ui.adsabs.harvard.edu/abs/2012PhRvB..86j0506R). doi:10.1103/physrevb.86.100506 (https://doi.org/10.1103%2Fphysrevb.86.100506). ISSN 1098-0121 (https://search.worldcat.org/issn/1098-0121). S2CID 118702797 (https://api.semanticscholar.org/CorpusID:118702797).
8. Place, Alexander P. M.; Rodgers, Lila V. H.; Mundada, Pranav; Smitham, Basil M.; Fitzpatrick, Mattias; Leng, Zhaoqi; Premkumar, Anjali; Bryon, Jacob; Vrajitoarea, Andrei; Sussman, Sara; Cheng, Guangming; Madhavan, Trisha; Cava, Robert J.; de Leon, Nathalie; Houck, Andrew A. (2021-03-19). "New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7979772). *Nature Communications*. **12** (1): 1779. arXiv:2003.00024 (https://arxiv.org/abs/2003.00024). Bibcode:2021NatCo..12.1779P (https://ui.adsabs.harvard.edu/abs/2021NatCo..12.1779P). doi:10.1038/s41467-021-22030-5 (https://doi.org/10.1038%2Fs41467-021-22030-5). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 7979772 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7979772). PMID 33741989 (https://pubmed.ncbi.nlm.nih.gov/33741989).
9. Bouchiat, V.; Vion, D.; Joyez, P.; Esteve, D.; Devoret, M. H. (1998). "Quantum coherence with a single Cooper pair". *Physica Scripta*. **1998** (T76): 165. Bibcode:1998PhST...76..165B (https://ui.adsabs.harvard.edu/abs/1998PhST...76..165B). doi:10.1238/Physica.Topical.076a00165 (https://doi.org/10.1238%2FPhysica.Topical.076a00165). ISSN 1402-4896 (https://search.worldcat.org/issn/1402-4896). S2CID 250887469 (https://api.semanticscholar.org/CorpusID:250887469).
10. Yurtalan, M. A.; Shi, J.; Kononenko, M.; Lupascu, A.; Ashhab, S. (2020-10-27). "Implementation of a Walsh-Hadamard Gate in a Superconducting Qutrit" (https://link.aps.org/doi/10.1103/PhysRevLett.125.180504). *Physical Review Letters*. **125** (18): 180504. arXiv:2003.04879 (https://arxiv.org/abs/2003.04879). Bibcode:2020PhRvL.125r0504Y (https://ui.adsabs.harvard.edu/abs/2020PhRvL.125r0504Y). doi:10.1103/PhysRevLett.125.180504 (https://doi.org/10.1103%2FPhysRevLett.125.180504). PMID 33196217 (https://pubmed.ncbi.nlm.nih.gov/33196217). S2CID 128064435 (https://api.semanticscholar.org/CorpusID:128064435).
11. Morvan, A.; Ramasesh, V. V.; Blok, M. S.; Kreikebaum, J. M.; O'Brien, K.; Chen, L.; Mitchell, B. K.; Naik, R. K.; Santiago, D. I.; Siddiqi, I. (2021-05-27). "Qutrit Randomized Benchmarking" (https://link.aps.org/doi/10.1103/PhysRevLett.126.210504). *Physical Review Letters*. **126** (21): 210504. arXiv:2008.09134 (https://arxiv.org/abs/2008.09134). Bibcode:2021PhRvL.126u0504M (https://ui.adsabs.harvard.edu/abs/2021PhRvL.126u0504M). doi:10.1103/PhysRevLett.126.210504 (https://doi.org/10.1103%2FPhysRevLett.126.210504). hdl:1721.1/143809 (https://hdl.handle.net/1721.1%2F143809). PMID 34114846 (https://pubmed.ncbi.nlm.nih.gov/34114846). S2CID 221246177 (https://api.semanticscholar.org/CorpusID:221246177).

12. Goss, Noah; Morvan, Alexis; Marinelli, Brian; Mitchell, Bradley K.; Nguyen, Long B.; Naik, Ravi K.; Chen, Larry; Jünger, Christian; Kreikebaum, John Mark; Santiago, David I.; Wallman, Joel J.; Siddiqi, Irfan (2022-12-05). "High-fidelity qutrit entangling gates for superconducting circuits" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9722686). *Nature Communications*. **13** (1): 7481. arXiv:2206.07216 (https://arxiv.org/abs/2206.07216). Bibcode:2022NatCo..13.7481G (https://ui.adsabs.harvard.edu/abs/2022NatCo..13.7481G). doi:10.1038/s41467-022-34851-z (https://doi.org/10.1038%2Fs41467-022-34851-z). ISSN 2041-1723 (https://search.worldcat.org/issn/2041-1723). PMC 9722686 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9722686). PMID 36470858 (https://pubmed.ncbi.nlm.nih.gov/36470858).
13. Fischer, Laurin E.; Chiesa, Alessandro; Tacchino, Francesco; Egger, Daniel J.; Carretta, Stefano; Tavernelli, Ivano (2023-08-28). "Universal Qudit Gate Synthesis for Transmons" (https://link.aps.org/doi/10.1103/PRXQuantum.4.030327). *PRX Quantum*. **4** (3): 030327. arXiv:2212.04496 (https://arxiv.org/abs/2212.04496). Bibcode:2023PRXQ....4c0327F (https://ui.adsabs.harvard.edu/abs/2023PRXQ....4c0327F). doi:10.1103/PRXQuantum.4.030327 (https://doi.org/10.1103%2FPRXQuantum.4.030327). S2CID 254408561 (https://api.semanticscholar.org/CorpusID:254408561).

Retrieved from "https://en.wikipedia.org/w/index.php?title=Transmon&oldid=1204900952"

WIKIPEDIA
The Free Encyclopedia

Quantum programming

Quantum programming is the process of designing or assembling sequences of instructions, called quantum circuits, using gates, switches, and operators to manipulate a quantum system for a desired outcome or results of a given experiment. Quantum circuit algorithms can be implemented on integrated circuits, conducted with instrumentation, or written in a programming language for use with a quantum computer or a quantum processor.

With quantum processor based systems, quantum programming languages help express quantum algorithms using high-level constructs.[1] The field is deeply rooted in the open-source philosophy and as a result most of the quantum software discussed in this article is freely available as open-source software.[2]

Quantum computers, such as those based on the KLM protocol, a linear optical quantum computing (LOQC) model, use quantum algorithms (circuits) implemented with electronics, integrated circuits, instrumentation, sensors, and/or by other physical means.

Other circuits designed for experimentation related to quantum systems can be instrumentation and sensor based.

Quantum instruction sets

Quantum instruction sets are used to turn higher level algorithms into physical instructions that can be executed on quantum processors. Sometimes these instructions are specific to a given hardware platform, e.g. ion traps or superconducting qubits.

Blackbird

Blackbird[3][4] is a quantum instruction set and intermediate representation used by Xanadu Quantum Technologies and Strawberry Fields. It is designed to represent continuous-variable quantum programs that can run on photonic quantum hardware.

cQASM

cQASM,[5] also known as common QASM, is a hardware-agnostic quantum assembly language which guarantees the interoperability between all the quantum compilation and simulation tools. It was introduced by the QCA Lab at TUDelft.

OpenQASM

OpenQASM[6] is the intermediate representation introduced by IBM for use with Qiskit and the IBM Q Experience.

Quil

Quil is an instruction set architecture for quantum computing that first introduced a shared quantum/classical memory model. It was introduced by Robert Smith, Michael Curtis, and William Zeng in *A Practical Quantum Instruction Set Architecture*.[7] Many quantum algorithms (including quantum teleportation, quantum error correction, simulation,[8][9] and optimization algorithms[10]) require a shared memory architecture.

Quantum software development kits

Quantum software development kits provide collections of tools to create and manipulate quantum programs.[11] They also provide the means to simulate the quantum programs or prepare them to be run using cloud-based quantum devices and self-hosted quantum devices.

SDKs with access to quantum processors

The following software development kits can be used to run quantum circuits on prototype quantum devices, as well as on simulators.

Cirq

An open source project developed by Google, which uses the Python programming language to create and manipulate quantum circuits. Programs written in Cirq can be run on IonQ, Pasqal,[12] Rigetti, and Alpine Quantum Technologies.[13]

Classiq

A cloud-based quantum IDE developed by Classiq, uses a high-level quantum language, Qmod, to generate scalable and efficient quantum circuits with a hardware-aware synthesis engine, that can be deployed across a wide range of QPUs. The platform includes a large library of quantum algorithms.

Forest

An open source project developed by Rigetti, which uses the Python programming language to create and manipulate quantum circuits. Results are obtained either using simulators or prototype quantum devices provided by Rigetti. As well as the ability to create programs using basic quantum operations, higher level algorithms are available within the Grove package.[14] Forest is based on the Quil instruction set.

MindQuantum

MindQuantum is a quantum computing framework based on MindSpore, focusing on the implementation of NISQ algorithms.[15][16][17]

Ocean

An open source suite of tools developed by D-Wave. Written mostly in the Python programming language, it enables users to formulate problems in Ising Model and Quadratic Unconstrained Binary Optimization formats (QUBO). Results can be obtained by submitting to an online quantum computer in Leap, D-Wave's real-time Quantum Application Environment, customer-owned machines, or classical samplers.

PennyLane

An open-source Python library developed by Xanadu Quantum Technologies for differentiable programming of quantum computers.[18][19][20][21] PennyLane provides users the ability to create models using TensorFlow, NumPy, or PyTorch, and connect them with quantum computer backends available from IBMQ, Google Quantum, Rigetti, Quantinuum[22] and Alpine Quantum Technologies.[13][23]

```python
from projectq import MainEngine        # import the main compiler engine
from projectq.ops import H, Measure, X # import the operations we want to
                                       # perform (Hadamard, X, measurement)

eng = MainEngine()   # create a default compiler (the backend is a simulator)
qubit = eng.allocate_qubit() # allocate 1 qubit

H | qubit # apply a Hadamard gate
X | qubit # apply an X gate
Measure | qubit # measure the qubit

eng.flush() # flush all gates (and execute measurements)
print("Measured {}".format(int(qubit))) # output measurement result

#
# Output: "Measured 1"
#
# Note that this is the (slow) Python simulator.
```

A sample code using projectq with Python

Perceval

An open-source project created by Quandela for designing photonic quantum circuits and developing quantum algorithms, based on Python. Simulations are run either on the user's own computer or on the cloud. Perceval is also used to connect to Quandela's cloud-based photonic quantum processor.[24][25]

ProjectQ

An open source project developed at the Institute for Theoretical Physics at ETH, which uses the Python programming language to create and manipulate quantum circuits.[26] Results are obtained either using a simulator, or by sending jobs to IBM quantum devices.

Qibo

An open source full-stack API for quantum simulation, quantum hardware control and calibration developed by multiple research laboratories, including QRC, CQT and INFN. Qibo (https://github.com/qiboteam/qibo) is a modular framework which includes multiple backends for quantum simulation and hardware control.[27][28] This project aims at providing a platform agnostic quantum hardware control framework with drivers for multiple instruments[29] and tools for quantum calibration, characterization and validation.[30] This framework focuses on self-hosted quantum devices by simplifying the software development required in labs.

Qiskit

An open source project developed by IBM.[31] Quantum circuits are created and manipulated using Python. Results are obtained either using simulators that run on the user's own device, simulators provided by IBM or prototype quantum devices provided by IBM. As well as the ability to create

programs using basic quantum operations, higher level tools for algorithms and benchmarking are available within specialized packages.[32] Qiskit is based on the OpenQASM standard for representing quantum circuits. It also supports pulse level control of quantum systems via QiskitPulse standard.[33]

Qrisp

Qrisp[34] is an open source project coordinated by the Eclipse Foundation[35] and developed in Python programming by Fraunhofer FOKUS[36] Qrisp is a high-level programming language for creating and compiling quantum algorithms. Its structured programming model enables scalable development and maintenance. The expressive syntax is based on variables instead of qubits, with the QuantumVariable as core class, and functions instead of gates. Additional tools, such as a performant simulator and automatic uncomputation, complement the extensive framework. Furthermore, it is platform independent, since it offers alternative compilation of elementary functions down to the circuit level, based on device-specific gate sets.

Quantum Development Kit

A project developed by Microsoft[37] as part of the .NET Framework. Quantum programs can be written and run within Visual Studio and VSCode using the quantum programming language Q#. Programs developed in the QDK can be run on Microsoft's Azure Quantum,[38] and run on quantum computers from Quantinuum,[22] IonQ, and Pasqal.[12]

Strawberry Fields

An open-source Python library developed by Xanadu Quantum Technologies for designing, simulating, and optimizing continuous variable (CV) quantum optical circuits.[39][40] Three simulators are provided - one in the Fock basis, one using the Gaussian formulation of quantum optics,[41] and one using the TensorFlow machine learning library. Strawberry Fields is also the library for executing programs on Xanadu's quantum photonic hardware.[42][43]

t|ket>

A quantum programming environment and optimizing compiler developed by Cambridge Quantum Computing that targets simulators and several quantum hardware back-ends, released in December 2018.[44]

Quantum programming languages

There are two main groups of quantum programming languages: imperative quantum programming languages and functional quantum programming languages.

Imperative languages

The most prominent representatives of the imperative languages are QCL,[45] LanQ[46] and Q|SI>.[47]

Ket

Ket[48] is an open-source embedded language designed to facilitate quantum programming, leveraging the familiar syntax and simplicity of Python. It serves as an integral component of the Ket Quantum Programming Platform,[49] seamlessly integrating with a Rust runtime library and a quantum simulator. Maintained by Quantuloop, the project emphasizes accessibility and versatility for researchers and developers. The following example demonstrates the implementation of a Bell state using Ket:

```
from ket import *
a, b = quant(2) # Allocate two quantum bits
H(a) # Put qubit `a` in a superposition
cnot(a, b) # Entangle the two qubits in the Bell state
m_a = measure(a) # Measure qubit `a`, collapsing qubit `b` as well
m_b = measure(b) # Measure qubit `b`
# Assert that the measurement of both qubits will always be equal
assert m_a.value == m_b.value
```

LQP

The Logic of Quantum Programs (LQP) is a dynamic quantum logic, capable of expressing important features of quantum measurements and unitary evolutions of multi-partite states, and provides logical characterizations of various forms of entanglement. The logic has been used to specify and verify the correctness of various protocols in quantum computation.[50][51]

Q language

Q Language is the second implemented imperative quantum programming language.[52] Q Language was implemented as an extension of C++ programming language. It provides classes for basic quantum operations like QHadamard, QFourier, QNot, and QSwap, which are derived from the base class Qop. New operators can be defined using C++ class mechanism.

Quantum memory is represented by class Qreg.

```
Qreg x1; // 1-qubit quantum register with initial value 0
Qreg x2(2,0); // 2-qubit quantum register with initial value 0
```

The computation process is executed using a provided simulator. Noisy environments can be simulated using parameters of the simulator.

Q#

A language developed by Microsoft to be used with the Quantum Development Kit.[53]

QCL

Quantum Computation Language (QCL) is one of the first implemented quantum programming languages.[54] The most important feature of QCL is the support for user-defined operators and functions. Its syntax resembles the syntax of the C programming language and its classical data types are similar to primitive data types in C. One can combine classical code and quantum code in the same program.

qGCL

Quantum Guarded Command Language (qGCL) was defined by P. Zuliani in his PhD thesis. It is based on Guarded Command Language created by Edsger Dijkstra.

It can be described as a language of quantum programs specification.

QMASM

Quantum Macro Assembler (QMASM) is a low-level language specific to quantum annealers such as the D-Wave.[55]

Qmod

Quantum Modeling (Qmod) language is a high-level language that abstracts away the gate-level qubit operation, providing a functional approach to the implementation of quantum algorithms on quantum registers. The language is part of the Classiq (https://classiq.io) platform and can be used directly with its native syntax, through a Python SDK, or with a visual editor, all methods can take advantage of the larger library of algorithms and the efficient circuit optimization.

Q|SI>

Q|SI> is a platform embedded in .Net language supporting quantum programming in a quantum extension of while-language.[47][56] This platform includes a compiler of the quantum while-language[57] and a chain of tools for the simulation of quantum computation, optimisation of quantum circuits, termination analysis of quantum programs,[58] and verification of quantum programs.[59][60]

Quantum pseudocode

Quantum pseudocode proposed by E. Knill is the first formalized language for description of quantum algorithms. It was introduced and, moreover, was tightly connected with a model of quantum machine called Quantum Random Access Machine (QRAM).

Scaffold

Scaffold is C-like language, that compiles to QASM and OpenQASM. It is built on top of the LLVM Compiler Infrastructure to perform optimizations on Scaffold code before generating a specified instruction set.[61][62]

Silq

Silq is a high-level programming language for quantum computing with a strong static type system, developed at ETH Zürich.[63][64]

Functional languages

Efforts are underway to develop functional programming languages for quantum computing. Functional programming languages are well-suited for reasoning about programs. Examples include Selinger's QPL,[65] and the Haskell-like language QML by Altenkirch and Grattage.[66][67] Higher-order quantum programming languages, based on lambda calculus, have been proposed by van Tonder,[68] Selinger and Valiron[69] and by Arrighi and Dowek.[70]

LIQUi|>

LIQUi|> (pronounced *liquid*) is a quantum simulation extension on the F# programming language.[71] It is currently being developed by the Quantum Architectures and Computation Group (QuArC)[72] part of the StationQ efforts at Microsoft Research. LIQUi|> seeks to allow theorists to experiment with quantum algorithm design before physical quantum computers are available for use.[73]

It includes a programming language, optimization and scheduling algorithms, and quantum simulators. LIQUi|> can be used to translate a quantum algorithm written in the form of a high-level program into the low-level machine instructions for a quantum device.[74]

QFC and QPL

QFC and QPL are two closely related quantum programming languages defined by Peter Selinger. They differ only in their syntax: QFC uses a flow chart syntax, whereas QPL uses a textual syntax. These languages have classical control flow but can operate on quantum or classical data. Selinger gives a denotational semantics for these languages in a category of superoperators.

QML

QML is a Haskell-like quantum programming language by Altenkirch and Grattage.[75][66] Unlike Selinger's QPL, this language takes duplication, rather than discarding, of quantum information as a primitive operation. Duplication in this context is understood to be the operation that maps $|\phi\rangle$ to $|\phi\rangle \otimes |\phi\rangle$, and is not to be confused with the impossible operation of cloning; the authors claim it is akin to how sharing is modeled in classical languages. QML also introduces both classical and quantum control operators, whereas most other languages rely on classical control.

An operational semantics for QML is given in terms of quantum circuits, while a denotational semantics is presented in terms of superoperators, and these are shown to agree. Both the operational and denotational semantics have been implemented (classically) in Haskell.[76]

Quantum lambda calculi

Quantum lambda calculi are extensions of the classical lambda calculus introduced by Alonzo Church and Stephen Cole Kleene in the 1930s. The purpose of quantum lambda calculi is to extend quantum programming languages with a theory of higher-order functions.

The first attempt to define a quantum lambda calculus was made by Philip Maymin in 1996.[77] His lambda-q calculus is powerful enough to express any quantum computation. However, this language can efficiently solve NP-complete problems, and therefore appears to be strictly stronger than the standard

quantum computational models (such as the quantum Turing machine or the quantum circuit model). Therefore, Maymin's lambda-q calculus is probably not implementable on a physical device .

In 2003, André van Tonder defined an extension of the lambda calculus suitable for proving correctness of quantum programs. He also provided an implementation in the Scheme programming language.[78]

In 2004, Selinger and Valiron defined a strongly typed lambda calculus for quantum computation with a type system based on linear logic.[79]

Quipper

Quipper was published in 2013.[80][81] It is implemented as an embedded language, using Haskell as the host language.[82] For this reason, quantum programs written in Quipper are written in Haskell using provided libraries. For example, the following code implements preparation of a superposition

```
import Quipper

spos :: Bool -> Circ Qubit
spos b = do q <- qinit b
            r <- hadamard q
            return r
```

References

1. Jarosław Adam Miszczak (2012). *High-level Structures in Quantum Computing*. Morgan & Claypool Publishers. ISBN 9781608458516.
2. "Comprehensive list of quantum open-source projects" (https://github.com/qosf/awesome-quantum-software). *Github*. Retrieved January 27, 2022.
3. "Blackbird Quantum Assembly Language — Blackbird 0.2.0 documentation" (https://quantum-blackbird.readthedocs.io/en/latest/). *quantum-blackbird.readthedocs.io*. Retrieved June 24, 2019.
4. Weedbrook, Christian; Amy, Matthew; Bergholm, Ville; Quesada, Nicolás; Izaac, Josh; Killoran, Nathan (March 11, 2019). "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum*. **3**: 129. arXiv:1804.03159 (https://arxiv.org/abs/1804.03159). Bibcode:2019Quant...3..129K (https://ui.adsabs.harvard.edu/abs/2019Quant...3..129K). doi:10.22331/q-2019-03-11-129 (https://doi.org/10.22331%2Fq-2019-03-11-129). S2CID 54763305 (https://api.semanticscholar.org/CorpusID:54763305).
5. Bertels, K.; Almudever, C. G.; Hogaboam, J. W.; Ashraf, I.; Guerreschi, G. G.; Khammassi, N. (May 24, 2018). "cQASM v1.0: Towards a Common Quantum Assembly Language". arXiv:1805.09607v1 (https://arxiv.org/abs/1805.09607v1) [quant-ph (https://arxiv.org/archive/quant-ph)].
6. *qiskit-openqasm: OpenQASM specification* (https://github.com/IBM/qiskit-openqasm), International Business Machines, July 4, 2017, retrieved July 6, 2017
7. Smith, Robert S.; Curtis, Michael J.; Zeng, William J. (2016). "A Practical Quantum Instruction Set Architecture". arXiv:1608.03355 (https://arxiv.org/abs/1608.03355) [quant-ph (https://arxiv.org/archive/quant-ph)].

8. McClean, Jarrod R.; Romero, Jonathan; Babbush, Ryan; Aspuru-Guzik, Alán (February 4, 2016). "The theory of variational hybrid quantum-classical algorithms". *New Journal of Physics*. **18** (2): 023023. arXiv:1509.04279 (https://arxiv.org/abs/1509.04279). Bibcode:2016NJPh...18b3023M (https://ui.adsabs.harvard.edu/abs/2016NJPh...18b3023M). doi:10.1088/1367-2630/18/2/023023 (https://doi.org/10.1088%2F1367-2630%2F18%2F2%2F023023). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 92988541 (https://api.semanticscholar.org/CorpusID:92988541).
9. Rubin, Nicholas C.; Curtis, Michael J.; Zeng, William J. (2016). "A Hybrid Classical/Quantum Approach for Large-Scale Studies of Quantum Systems with Density Matrix Embedding Theory". arXiv:1610.06910 (https://arxiv.org/abs/1610.06910) [quant-ph (https://arxiv.org/archive/quant-ph)].
10. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
11. Häner, Thomas; Steiger, Damian S.; Svore, Krysta; Troyer, Matthias (2018). "A software methodology for compiling quantum programs". *Quantum Science and Technology*. **3** (2): 020501. arXiv:1604.01401 (https://arxiv.org/abs/1604.01401). Bibcode:2018QS&T....3b0501H (https://ui.adsabs.harvard.edu/abs/2018QS&T....3b0501H). doi:10.1088/2058-9565/aaa5cc (https://doi.org/10.1088%2F2058-9565%2Faaa5cc). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 1922315 (https://api.semanticscholar.org/CorpusID:1922315).
12. "PASQAL" (https://pasqal.io/). *PASQAL*.
13. "Home" (https://www.aqt.eu/). *AQT | ALPINE QUANTUM TECHNOLOGIES*.
14. "Welcome to the Documentation for Grove! — Grove 1.7.0 documentation" (https://grove-docs.readthedocs.io/en/latest/). *grove-docs.readthedocs.io*.
15. "MindSpore Quantum Documentation" (https://www.mindspore.cn/mindquantum/docs/en/master/index.html). *www.mindspore.cn/mindquantum*.
16. Xu, Xusheng; et al. (2024). "MindSpore Quantum: A User-Friendly, High-Performance, and AI-Compatible Quantum Computing Framework". arXiv:2406.17248 (https://arxiv.org/abs/2406.17248) [quant-ph (https://arxiv.org/archive/quant-ph)].
17. "mindquantum" (https://github.com/mindspore-ai/mindquantum). *github.com*.
18. "PennyLane Documentation — PennyLane 0.14.1 documentation" (https://pennylane.readthedocs.io/en/stable/). *pennylane.readthedocs.io*. Retrieved March 26, 2021.
19. "AWS joins PennyLane, an open-source framework that melds machine learning with quantum computing" (https://siliconangle.com/2021/02/17/aws-throws-weight-behind-pennylane-open-source-framework-melds-machine-learning-quantum-computing/). *SiliconANGLE*. February 17, 2021. Retrieved March 26, 2021.
20. "SD Times Open-Source Project of the Week: PennyLane" (https://sdtimes.com/open-source/sd-times-open-source-project-of-the-week-pennylane/). *SD Times*. February 26, 2021. Retrieved March 26, 2021.
21. Salamone, Salvatore (December 13, 2020). "Real-time Analytics News Roundup for Week Ending December 12" (https://www.rtinsights.com/real-time-analytics-news-roundup-for-week-ending-december-12/). *RTInsights*. Retrieved March 26, 2021.
22. "Accelerating Quantum Computing" (https://www.quantinuum.com/). *www.quantinuum.com*.
23. "Plugins and ecosystem — PennyLane" (https://pennylane.ai/plugins.html). *pennylane.ai*. Retrieved March 26, 2021.
24. "La puissance d'un ordinateur quantique testée en ligne (The power of a quantum computer tested online)" (https://www.lemonde.fr/sciences/article/2022/11/22/la-puissance-d-un-ordinateur-quantique-testee-en-ligne_6151063_1650684.html). *Le Monde.fr*. Le Monde. November 22, 2022.

25. Heurtel, Nicolas; Fyrillas, Andreas; de Gliniasty, Grégoire; Le Bihan, Raphaël; Malherbe, Sébastien; Pailhas, Marceau; Bertasi, Eric; Bourdoncle, Boris; Emeriau, Pierre-Emmanuel; Mezher, Rawad; Music, Luka; Belabas, Nadia; Valiron, Benoît; Senellart, Pascale; Mansfield, Shane; Senellart, Jean (February 21, 2023). "Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing" (https://quantum-journal.org/papers/q-2023-02-21-931/). *Quantum*. **7**: 931. arXiv:2204.00602 (https://arxiv.org/abs/2204.00602). Bibcode:2023Quant...7..931H (https://ui.adsabs.harvard.edu/abs/2023Quant...7..931H). doi:10.22331/q-2023-02-21-931 (https://doi.org/10.22331%2Fq-2023-02-21-931). S2CID 247922568 (https://api.semanticscholar.org/CorpusID:247922568).
26. "Home" (https://projectq.ch/).
27. Efthymiou, Stavros; Ramos-Calderer, Sergi; Bravo-Prieto, Carlos; Pérez-Salinas, Adrián; García-Martín, Diego; Garcia-Saez, Artur; Latorre, José Ignacio; Carrazza, Stefano (January 1, 2022). "Qibo: a framework for quantum simulation with hardware acceleration" (https://iopscience.iop.org/article/10.1088/2058-9565/ac39f5). *Quantum Science and Technology*. **7** (1): 015018. arXiv:2009.01845 (https://arxiv.org/abs/2009.01845). Bibcode:2022QS&T....7a5018E (https://ui.adsabs.harvard.edu/abs/2022QS&T....7a5018E). doi:10.1088/2058-9565/ac39f5 (https://doi.org/10.1088%2F2058-9565%2Fac39f5). hdl:2434/887963 (https://hdl.handle.net/2434%2F887963). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 221507478 (https://api.semanticscholar.org/CorpusID:221507478).
28. Efthymiou, Stavros; Lazzarin, Marco; Pasquale, Andrea; Carrazza, Stefano (September 22, 2022). "Quantum simulation with just-in-time compilation" (https://quantum-journal.org/papers/q-2022-09-22-814/). *Quantum*. **6**: 814. arXiv:2203.08826 (https://arxiv.org/abs/2203.08826). Bibcode:2022Quant...6..814E (https://ui.adsabs.harvard.edu/abs/2022Quant...6..814E). doi:10.22331/q-2022-09-22-814 (https://doi.org/10.22331%2Fq-2022-09-22-814). S2CID 247518955 (https://api.semanticscholar.org/CorpusID:247518955).
29. "Qibolab" (https://github.com/qiboteam/qibolab). November 2, 2022 – via GitHub.
30. "Qibocal" (https://github.com/qiboteam/qibocal). November 1, 2022 – via GitHub.
31. "qiskit.org" (https://qiskit.org/). *qiskit.org*.
32. "Qiskit Overview" (https://qiskit.org/overview/). Retrieved February 10, 2021.
33. McKay, David C.; Alexander, Thomas; Bello, Luciano; Biercuk, Michael J.; Bishop, Lev; Chen, Jiayin; Chow, Jerry M.; Córcoles, Antonio D.; Egger, Daniel; Filipp, Stefan; Gomez, Juan; Hush, Michael; Javadi-Abhari, Ali; Moreda, Diego; Nation, Paul; Paulovicks, Brent; Winston, Erick; Wood, Christopher J.; Wootton, James; Gambetta, Jay M. (2018). "Qiskit Backend Specifications for OpenQASM and OpenPulse Experiments". arXiv:1809.03452 (https://arxiv.org/abs/1809.03452) [quant-ph (https://arxiv.org/archive/quant-ph)].
34. "Qrisp official website" (https://www.qrisp.eu/).
35. "Eclipse Foundation (website)" (https://www.eclipse.org/org/foundation/).
36. "Fraunhofer FOKUS (website)" (https://www.fokus.fraunhofer.de/).
37. "Azure Quantum documentation, QDK & Q# API reference - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/). *learn.microsoft.com*.
38. "What is Azure Quantum? - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum). *learn.microsoft.com*. January 11, 2023.
39. "Strawberry Fields — Strawberry Fields 0.8.0 documentation" (https://strawberryfields.readthedocs.io/en/latest/). *strawberryfields.readthedocs.io*. Retrieved September 25, 2018.
40. Killoran, Nathan; Izaac, Josh; Quesada, Nicolás; Bergholm, Ville; Amy, Matthew; Weedbrook, Christian (2019). "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum*. **3**: 129. arXiv:1804.03159 (https://arxiv.org/abs/1804.03159). Bibcode:2019Quant...3..129K (https://ui.adsabs.harvard.edu/abs/2019Quant...3..129K). doi:10.22331/q-2019-03-11-129 (https://doi.org/10.22331%2Fq-2019-03-11-129). S2CID 54763305 (https://api.semanticscholar.org/CorpusID:54763305).

41. Weedbrook, Christian; Pirandola, Stefano; García-Patrón, Raúl; Cerf, Nicolas J.; Ralph, Timothy C.; Shapiro, Jeffrey H.; Lloyd, Seth (May 1, 2012). "Gaussian quantum information". *Reviews of Modern Physics*. **84** (2): 621–669. arXiv:1110.3234 (https://arxiv.org/abs/1110.3234). Bibcode:2012RvMP...84..621W (https://ui.adsabs.harvard.edu/abs/2012RvMP...84..621W). doi:10.1103/RevModPhys.84.621 (https://doi.org/10.1103%2FRevModPhys.84.621). S2CID 119250535 (https://api.semanticscholar.org/CorpusID:119250535).
42. "Hardware — Strawberry Fields" (https://strawberryfields.ai/photonics/hardware/index.html). *strawberryfields.ai*. Retrieved March 26, 2021.
43. "In the Race to Hundreds of Qubits, Photons May Have "Quantum Advantage" " (https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon). *IEEE Spectrum: Technology, Engineering, and Science News*. March 5, 2021. Retrieved March 26, 2021.
44. "pytket" (https://github.com/CQCL/pytket). *GitHub*. January 22, 2022.
45. Bernhard Omer. "The QCL Programming Language" (http://tph.tuwien.ac.at/~oemer/qcl.html).
46. Hynek Mlnařík. "LanQ – a quantum imperative programming language" (http://lanq.sourceforge.net/).
47. Liu, Shusen; Zhou, li; Guan, Ji; He, Yang; Duan, Runyao; Ying, Mingsheng (May 9, 2017). "Q|SI>: A Quantum Programming Language". *Scientia Sinica Informationis*. **47** (10): 1300. arXiv:1710.09500 (https://arxiv.org/abs/1710.09500). doi:10.1360/N112017-00095 (https://doi.org/10.1360%2FN112017-00095). S2CID 9163705 (https://api.semanticscholar.org/CorpusID:9163705).
48. Da Rosa, Evandro Chagas Ribeiro; De Santiago, Rafael (January 31, 2022). "Ket Quantum Programming" (https://dl.acm.org/doi/10.1145/3474224). *ACM Journal on Emerging Technologies in Computing Systems*. **18** (1): 1–25. doi:10.1145/3474224 (https://doi.org/10.1145%2F3474224). ISSN 1550-4832 (https://search.worldcat.org/issn/1550-4832).
49. "Ket Quantum Programming" (https://quantumket.org). *quantumket.org*. Retrieved May 18, 2023.
50. A. Baltag and S. Smets, "LQP: The Dynamic Logic of Quantum Information" (https://arxiv.org/abs/2110.01361), Mathematical Structures in Computer Science 16(3):491-525, 2006.
51. Baltag, Alexandru; Bergfeld, Jort; Kishida, Kohei; Sack, Joshua; Smets, Sonja; Zhong, Shengyang (2014). "PLQP & Company: Decidable Logics for Quantum Algorithms" (https://link.springer.com/article/10.1007/s10773-013-1987-3). *International Journal of Theoretical Physics*. **53** (10): 3628–3647. Bibcode:2014IJTP...53.3628B (https://ui.adsabs.harvard.edu/abs/2014IJTP...53.3628B). doi:10.1007/s10773-013-1987-3 (https://doi.org/10.1007%2Fs10773-013-1987-3). S2CID 254573992 (https://api.semanticscholar.org/CorpusID:254573992).
52. "Software for the Q language" (https://web.archive.org/web/20090620011647/http://sra.itc.it/people/serafini/qlang/). November 23, 2001. Archived from the original (http://sra.itc.it/people/serafini/qlang/) on June 20, 2009. Retrieved July 20, 2017.
53. "Introduction to Q# & Quantum Development Kit - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk). *learn.microsoft.com*. March 30, 2023.
54. "QCL - A Programming Language for Quantum Computers" (http://tph.tuwien.ac.at/~oemer/qcl.html). *tuwien.ac.at*. Retrieved July 20, 2017.
55. Scott Pakin, "A Quantum Macro Assembler" (https://ieeexplore.ieee.org/document/7761637/), Proceedings of the 20th Annual IEEE High Performance Extreme Computing Conference 2016
56. Ying, Mingsheng (January 2012). "Floyd–hoare Logic for Quantum Programs" (https://doi.org/10.1145%2F2049706.2049708). *ACM Trans. Program. Lang. Syst*. **33** (6): 19:1–19:49. doi:10.1145/2049706.2049708 (https://doi.org/10.1145%2F2049706.2049708). ISSN 0164-0925 (https://search.worldcat.org/issn/0164-0925). S2CID 416960 (https://api.semanticscholar.org/CorpusID:416960).

57. Ying, Mingsheng; Feng, Yuan (2010). "A Flowchart Language for Quantum Programming" (https://www.computer.org/csdl/trans/ts/2011/04/tts2011040466-abs.html). *IEEE Transactions on Software Engineering*. **37** (4): 466–485. doi:10.1109/TSE.2010.94 (https://doi.org/10.1109%2FTSE.2010.94). ISSN 0098-5589 (https://search.worldcat.org/issn/0098-5589). S2CID 5879273 (https://api.semanticscholar.org/CorpusID:5879273).
58. Ying, Mingsheng; Yu, Nengkun; Feng, Yuan; Duan, Runyao (2013). "Verification of quantum programs". *Science of Computer Programming*. **78** (9): 1679–1700. arXiv:1106.4063 (https://arxiv.org/abs/1106.4063). doi:10.1016/j.scico.2013.03.016 (https://doi.org/10.1016%2Fj.scico.2013.03.016). S2CID 18913620 (https://api.semanticscholar.org/CorpusID:18913620).
59. Ying, Mingsheng; Ying, Shenggang; Wu, Xiaodi (2017), "Invariants of quantum programs: Characterisations and generation", *ACM SIGPLAN Notices*, **52**: 818–832, doi:10.1145/3093333.3009840 (https://doi.org/10.1145%2F3093333.3009840), hdl:10453/127333 (https://hdl.handle.net/10453%2F127333)
60. Liu, Tao; Li, Yangjia; Wang, Shuling; Ying, Mingsheng; Zhan, Naijun (2016). "A Theorem Prover for Quantum Hoare Logic and its Applications". arXiv:1601.03835 (https://arxiv.org/abs/1601.03835) [cs.LO (https://arxiv.org/archive/cs.LO)].
61. Javadi-Abhari, Ali. "Scaffold: Quantum Programming Language" (https://www.cs.princeton.edu/research/techreps/TR-934-12). *Princeton University-Department of Computer Science*. Princeton University. Retrieved September 22, 2020.
62. Litteken, Andrew (May 28, 2020). "An updated LLVM-based quantum research compiler with further OpenQASM support" (https://doi.org/10.1088%2F2058-9565%2Fab8c2c). *Quantum Science and Technology*. **5** (3): 034013. Bibcode:2020QS&T....5c4013L (https://ui.adsabs.harvard.edu/abs/2020QS&T....5c4013L). doi:10.1088/2058-9565/ab8c2c (https://doi.org/10.1088%2F2058-9565%2Fab8c2c). OSTI 1803951 (https://www.osti.gov/biblio/1803951). S2CID 219101628 (https://api.semanticscholar.org/CorpusID:219101628).
63. "What is Silq?" (https://silq.ethz.ch/). *silq.ethz.ch*. Retrieved June 21, 2020.
64. Bichsel, Benjamin; Baader, Maximilian; Gehr, Timon; Vechev, Martin (June 11, 2020). "Silq: A high-level quantum language with safe uncomputation and intuitive semantics". *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*. London UK: ACM. pp. 286–300. doi:10.1145/3385412.3386007 (https://doi.org/10.1145%2F3385412.3386007). ISBN 978-1-4503-7613-6. S2CID 219397029 (https://api.semanticscholar.org/CorpusID:219397029).
65. Peter Selinger, "Towards a quantum programming language" (http://www.mathstat.dal.ca/~selinger/papers.html#qpl), Mathematical Structures in Computer Science 14(4):527-586, 2004.
66. Jonathan Grattage: QML Research (http://www.cs.nott.ac.uk/~jjg/qml.html) (website)
67. T. Altenkirch, V. Belavkin, J. Grattage, A. Green, A. Sabry, J. K. Vizzotto, QML: A Functional Quantum Programming Language (http://sneezy.cs.nott.ac.uk/qml) Archived (https://web.archive.org/web/20060710201728/http://sneezy.cs.nott.ac.uk/QML/) 2006-07-10 at the Wayback Machine (website)
68. Andre van Tonder, "A Lambda Calculus for Quantum Computation" (https://dx.doi.org/10.1137/S0097539703432165), SIAM J. Comput., 33(5), 1109–1135. (27 pages), 2004. Also available from arXiv:quant-ph/0307150 (https://arxiv.org/abs/quant-ph/0307150)
69. Peter Selinger and Benoît Valiron, "A lambda calculus for quantum computation with classical control" (http://www.mathstat.dal.ca/~selinger/papers/#qlambda), Mathematical Structures in Computer Science 16(3):527-552, 2006.
70. Pablo Arrighi, Gilles Dowek, "Linear-algebraic lambda-calculus: higher-order, encodings and confluence" (http://www.arxiv.org/abs/quant-ph/0612199), 2006
71. "The Language Integrated Quantum Operations Simulator" (https://stationq.github.io/Liquid/). *github.io*. Retrieved July 20, 2017.
72. Quantum Architectures and Computation Group (QuArC), https://www.microsoft.com/en-us/research/group/quantum-architectures-and-computation-group-quarc/, 2011

73. "StationQ" (https://stationq.microsoft.com/). *microsoft.com*. Retrieved July 20, 2017.
74. "Language-Integrated Quantum Operations: LIQUi|>" (https://www.microsoft.com/en-us/research/project/language-integrated-quantum-operations-liqui/). *Microsoft*. 2016.
75. "QML: A Functional Quantum Programming Language" (https://web.archive.org/web/20070926230222/http://sneezy.cs.nott.ac.uk/QML/). September 26, 2007. Archived from the original (http://sneezy.cs.nott.ac.uk/QML/) on September 26, 2007.
76. Jonathan Grattage, QML: A Functional Quantum Programming Language (compiler) (http://sneezy.cs.nott.ac.uk/qml/compiler) Archived (https://web.archive.org/web/20160305052237/http://sneezy.cs.nott.ac.uk/qml/compiler/) 2016-03-05 at the Wayback Machine, 2005–2008
77. Philip Maymin, "Extending the Lambda Calculus to Express Randomized and Quantumized Algorithms" (https://arxiv.org/abs/quant-ph/9612052), 1996
78. André van Tonder. "A lambda calculus for quantum computation (website)" (https://web.archive.org/web/20160305100936/http://www.het.brown.edu/people/andre/qlambda/). Archived from the original (http://www.het.brown.edu/people/andre/qlambda) on March 5, 2016. Retrieved October 2, 2007.
79. Peter Selinger, Benoˆıt Valiron, "Quantum Lambda Calculus" (https://www.mscs.dal.ca/~selinger/papers/qlambdabook.pdf)
80. "The Quipper Language" (http://www.mathstat.dal.ca/~selinger/quipper/).
81. Alexander S. Green; Peter LeFanu Lumsdaine; Neil J. Ross; Peter Selinger; Benoît Valiron. "The Quipper Language (website)" (http://www.mathstat.dal.ca/~selinger/quipper/).
82. Alexander S. Green; Peter LeFanu Lumsdaine; Neil J. Ross; Peter Selinger; Benoît Valiron (2013). "An Introduction to Quantum Programming in Quipper". *Reversible Computation*. Lecture Notes in Computer Science. Vol. 7948. pp. 110–124. arXiv:1304.5485 (https://arxiv.org/abs/1304.5485). doi:10.1007/978-3-642-38986-3_10 (https://doi.org/10.1007%2F978-3-642-38986-3_10). ISBN 978-3-642-38985-6. S2CID 9135905 (https://api.semanticscholar.org/CorpusID:9135905).

Further reading

- Mingsheng, Ying (2024). *Foundations of quantum programming* (2nd ed.). Cambridge, Massachusetts: Morgan Kaufmann. ISBN 978-0-4431-5942-8. OCLC 1406095194 (https://search.worldcat.org/oclc/1406095194). 978-0-4431-5943-5 (eBook).
- Serrano, Manuel A.; Pérez-Castillo, Ricardo; Piattini, Mario, eds. (2022). *Quantum Software Engineering* (1st ed.). Cham, Switzerland: Springer. doi:10.1007/978-3-031-05324-5 (https://doi.org/10.1007%2F978-3-031-05324-5). ISBN 978-3-031-05323-8. OCLC 1347696597 (https://search.worldcat.org/oclc/1347696597). 978-3-031-05326-9 (softcover) & 978-3-031-05324-5 (eBook).

External links

- Curated list (https://github.com/qosf/awesome-quantum-software) of all quantum open-source software projects
- Bibliography on Quantum Programming Languages (http://www.dcs.gla.ac.uk/~simon/quantum/) (updated in May 2007)
- Quantum Physics and Logic (QPL) Conference Series (https://www.mathstat.dal.ca/~selinger/qpl/) (L stood for 'Languages' until 2006)
- Quantum programming language (https://quantiki.org/wiki/quantum-programming-language) in Quantiki (http://www.quantiki.org/)
- QMASM documentation (https://github.com/lanl/qmasm/wiki)

- pyQuil documentation (https://pyquil.readthedocs.io/en/stable/index.html) including Introduction to Quantum Computing (https://pyquil.readthedocs.io/en/stable/intro.html) Archived (https://web.archive.org/web/20180718165337/https://pyquil.readthedocs.io/en/stable/intro.html) July 18, 2018, at the Wayback Machine
- Scaffold Source (https://github.com/epiqc/ScaffCC)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_programming&oldid=1241083092"

WIKIPEDIA
The Free Encyclopedia

OpenQASM

Open Quantum Assembly Language (**OpenQASM**; pronounced *open kazm*[1]) is a programming language designed for describing quantum circuits and algorithms for execution on quantum computers. It is designed to be an intermediate representation that can be used by higher-level compilers to communicate with quantum hardware, and allows for the description of a wide range of quantum operations, as well as classical feed-forward flow control based on measurement outcomes.

OpenQASM

License	Apache License 2.0
Filename extensions	`.qasm`
Website	openqasm.com (https://openqasm.com/)

The language includes a mechanism for describing explicit timing of instructions, and allows for the attachment of low-level definitions to gates for tasks such as calibration.[1] OpenQASM is not intended for general-purpose classical computation, and hardware implementations of the language may not support the full range of data manipulation described in the specification. Compilers for OpenQASM are expected to support a wide range of classical operations for compile-time constants, but the support for these operations on runtime values may vary between implementations.[2]

The language was first described in a paper published in July 2017,[1] and a reference source code implementation was released as part of IBM's Quantum Information Software Kit (Qiskit) for use with their IBM Quantum Experience cloud quantum computing platform.[3] The language has similar qualities to traditional hardware description languages such as Verilog.

OpenQASM defines its version at the head of a source file as a number, as in the declaration:

```
OPENQASM 3;
```

The level of OpenQASM's original published implementations is OpenQASM 2.0. Version 3.0 of the specification is the current one and can be viewed at the OpenQASM (https://github.com/openqasm/openqasm) repository on *GitHub*.

Examples

The following is an example of OpenQASM source code from the official library. The program adds two four-bit numbers.[4]

```
/*
 * quantum ripple-carry adder
 * Cuccaro et al, quant-ph/0410184
 */
OPENQASM 3;
include "stdgates.inc";

gate majority a, b, c {
```

```
    cx c, b;
    cx c, a;
    ccx a, b, c;
}

gate unmaj a, b, c {
    ccx a, b, c;
    cx c, a;
    cx a, b;
}

qubit[1] cin;
qubit[4] a;
qubit[4] b;
qubit[1] cout;
bit[5] ans;
uint[4] a_in = 1;  // a = 0001
uint[4] b_in = 15; // b = 1111
// initialize qubits
reset cin;
reset a;
reset b;
reset cout;

// set input states
for i in [0: 3] {
  if(bool(a_in[i])) x a[i];
  if(bool(b_in[i])) x b[i];
}
// add a to b, storing result in b
majority cin[0], b[0], a[0];
for i in [0: 2] { majority a[i], b[i + 1], a[i + 1]; }
cx a[3], cout[0];
for i in [2: -1: 0] { unmaj a[i],b[i+1],a[i+1]; }
unmaj cin[0], b[0], a[0];
measure b[0:3] -> ans[0:3];
measure cout[0] -> ans[4];
```

References

1. Cross, Andrew W.; Bishop, Lev S.; Smolin, John A.; Gambetta, Jay M. (2017). "Open Quantum Assembly Language". arXiv:1707.03429 (https://arxiv.org/abs/1707.03429) [quant-ph (https://arxiv.org/archive/quant-ph)].
2. "OpenQASM Live Specification" (https://openqasm.com/intro.html). Retrieved 26 December 2022.
3. *qiskit-openqasm: OpenQASM specification* (https://qiskit.github.io/openqasm/), International Business Machines, 4 July 2017, retrieved 6 July 2017
4. "openqasm/adder.qasm at master · openqasm/openqasm · GitHub" (https://github.com/openqasm/openqasm/blob/main/examples/adder.qasm). *GitHub*. 29 January 2022.

External links

- Official website (https://openqasm.com/)
- openqasm (https://github.com/openqasm/openqasm) on GitHub

Retrieved from "https://en.wikipedia.org/w/index.php?title=OpenQASM&oldid=1226782594"

WIKIPEDIA
The Free Encyclopedia

Qiskit

Qiskit is an open-source software development kit (SDK) for working with quantum computers at the level of circuits, pulses, and algorithms. It provides tools for creating and manipulating quantum programs and running them on prototype quantum devices on IBM Quantum Platform or on simulators on a local computer. It follows the circuit model for universal quantum computation, and can be used for any quantum hardware (currently supports superconducting qubits and trapped ions)[4] that follows this model.

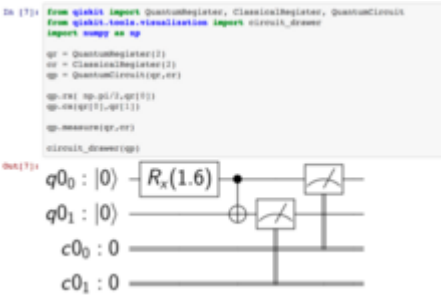
Qiskit was founded by IBM Research to allow software development for their cloud quantum computing service, IBM Quantum Experience.[5][6] Contributions are also made by external supporters, typically from academic institutions.[7][8]

The primary version of Qiskit uses the Python programming language. Versions for Swift[9] and JavaScript[10] were initially explored, though the development for these versions has halted. Instead, a minimal re-implementation of basic features is available as *MicroQiskit*,[11] which is made to be easy to port to alternative platforms.

A range of Jupyter notebooks are provided with examples of quantum computing being used.[12] Examples include the source code behind scientific studies that use Qiskit,[13] as well as a set of exercises to help people to learn the basics of quantum programming. An open source textbook based on Qiskit is available as a university-level quantum algorithms or quantum computation course supplement.[14]

Qiskit





Developer(s)	IBM Research, Qiskit community
Initial release	March 7, 2017.[1]
Stable release	0.45.0 / 3 November 2023[2]
Repository	github.com/Qiskit/qiskit (https://github.com/Qiskit/qiskit)
Written in	Python
Operating system	Cross-platform
Type	SDK for Quantum Computing
License	Apache License 2.0[3]
Website	qiskit.org (https://qiskit.org)

Components

Qiskit is made of elements that work together to enable quantum computing. The central goal of Qiskit is to build a software stack that makes it easier for anyone to use quantum computers, regardless of their skill level or area of interest; Qiskit allows users to design experiments and applications and run them on

real quantum computers and/or classical simulators. Qiskit provides the ability to develop quantum software both at the machine code level of OpenQASM, and at abstract levels suitable for end-users without quantum computing expertise. This functionality is provided by the following components.[15]

Qiskit Terra

The element Terra is the foundation on which the rest of Qiskit is built. Qiskit Terra provides tools to create quantum circuits at or close to the level of quantum machine code.[16] It allows the processes that run on quantum hardware to be explicitly constructed in terms of quantum gates. It also provides tools to allow quantum circuits to be optimized for a device, as well as managing batches of jobs and running them on remote-access quantum devices and simulators.

The following shows a simple example of Qiskit Terra. In this, a quantum circuit is created for two qubits, which consists of the quantum gates required to create a Bell state. The quantum circuit then ends with quantum measurements, which extract a bit from each qubit.

```
from qiskit import QuantumCircuit

qc = QuantumCircuit(2, 2)

qc.h(0)
qc.cx(0, 1)
qc.measure([0,1], [0,1])
```

Qiskit Aer

The element Aer provides high-performance quantum computing simulators with realistic noise models. In the near-term, development of quantum software will depend largely on simulation of small quantum devices. For Qiskit, this is provided by the Aer component. This provides simulators hosted locally on the user's device, as well as HPC resources available through the cloud.[17] The simulators can also simulate the effects of noise for simple and sophisticated noise models.[18]

Continuing with the previous example: Once the quantum circuit has been created, it can be run on a backend (either quantum hardware or a simulator). In the following example, a local simulator is used.

```
from qiskit import Aer, execute

backend = Aer.get_backend("qasm_simulator")
job = execute(qc, backend)
result = job.result()
print(result.get_counts(qc))
```

The final print statement here will show the results returned by the backend. This is a Python dictionary that describes the bit strings obtained from multiple runs of the quantum circuit. In the quantum circuit used in this example, the bit strings `'00'` and `'11'` should be the only possible results, and should occur with equal probability. The full results will therefore typically have the samples split approximately equally between the two, such as `{'00':519, '11':505}` .

Experiments done on quantum hardware using Qiskit have been used in many research papers,[19] such as in tests of quantum error correction,[20][21] generation of entanglement[22] and simulation of far-from-equilibrium dynamics.[23]

Qiskit Ignis

As of version 0.7.0, released on 6th December 2021, Qiskit Ignis has been deprecated and superseded by the Qiskit Experiments project.[24]

The element Ignis provides tools for quantum hardware verification, noise characterization, and error correction. Ignis is a component that contains tools for characterizing noise in near-term devices, as well as allowing computations to be performed in the presence of noise. This includes tools for benchmarking near-term devices, error mitigation and error correction.[25]

Ignis is meant for those who want to design quantum error correction codes, or who wish to study ways to characterize errors through methods such as tomography, or even to find a better way for using gates by exploring dynamical decoupling and optimal control.

Qiskit Aqua

As of version 0.9.0, released on 2nd April 2021, Qiskit Aqua has been deprecated with its support ending and eventual archival being no sooner than 3 months from that date.

The element Aqua provided a library of cross-domain algorithms upon which domain-specific applications can be built. However, the Qiskit 0.25.0 release included a restructuring of the applications and algorithms. What previously has been referred to as Qiskit Aqua, the single applications and algorithms module of Qiskit, is now split into dedicated application modules for Optimization, Finance, Machine Learning and Nature (including Physics & Chemistry). The core algorithms and opflow operator functionality were moved to Qiskit Terra.

Additionally, to the restructuring, all algorithms follow a unified paradigm: algorithms are classified according to the problems they solve, and within one application class algorithms can be used interchangeably to solve the same problem. This means that, unlike before, algorithm instances are decoupled from the problem they solve.[26]

Qiskit Optimization

Qiskit Optimization is an open-source framework that covers the whole range from high-level modeling of optimization problems, with automatic conversion of problems to different required representations, to a suite of easy-to-use quantum optimization algorithms that are ready to run on classical simulators, as well as on real quantum devices via Qiskit. The Optimization module enables easy, efficient modeling of optimization problems using docplex (https://developer.ibm.com/docloud/documentation/optimization-modeling/modeling-for-python/).[27]

Qiskit Finance

Qiskit Finance is an open-source framework that contains uncertainty components for stock/securities problems, Ising translators for portfolio optimizations and data providers to source real or random data to finance experiments.[28]

Qiskit Machine Learning

The Machine Learning package (as of 2021) contains sample datasets at present. It has some classification algorithms such as QSVM and VQC (Variational Quantum Classifier), where this data can be used for experiments, and there is also QGAN (Quantum Generative Adversarial Network) algorithm.[29]

Qiskit Nature

Qiskit Nature is an open-source framework that supports problems including ground state energy computations, excited states and dipole moments of molecule, both open and closed-shell. The code comprises chemistry drivers, which when provided with a molecular configuration will return one and two-body integrals as well as other data that is efficiently computed classically. This output data from a driver can then be used as input in Qiskit Nature that contains logic which is able to translate this into a form that is suitable for quantum algorithms.[30]

See also

- IBM Quantum Platform
- Cirq, Google's Quantum framework
- Quantum programming

References

1. Jay M. Gambetta; Andrew Cross (March 27, 2018). "Looking back on a year of Qiskit" (https://medium.com/qiskit/qiskit-turns-one-looking-back-cbc2c48d7a95). *Medium*. Archived (https://web.archive.org/web/20211216225930/https://medium.com/qiskit/qiskit-turns-one-looking-back-cbc2c48d7a95) from the original on December 16, 2021. Retrieved September 24, 2019.
2. "Releases – Qiskit" (https://github.com/Qiskit/qiskit/releases). *GitHub*. Archived (https://web.archive.org/web/20211216225948/https://github.com/Qiskit/qiskit/releases) from the original on 2021-12-16. Retrieved 2019-12-20.
3. License (https://github.com/Qiskit/qiskit-terra/blob/master/LICENSE.txt)
4. "Qiskit - Write once, target multiple architectures" (https://www.ibm.com/blogs/research/2019/11/qiskit-for-multiple-architectures/). *IBM Research Blog*. 2019-11-05. Archived (https://web.archive.org/web/20201126152348/https://www.ibm.com/blogs/research/2019/11/qiskit-for-multiple-architectures/) from the original on 2020-11-26. Retrieved 2019-12-20.
5. Magee, Tamlim (August 24, 2018). "What is Qiskit, IBM's open source quantum computing framework" (https://web.archive.org/web/20190306044548/https://www.computerworlduk.com/open-source/inside-qiskit-ibms-open-source-quantum-computing-framework-3682891/). *Computerworld UK*. Archived from the original (https://www.computerworlduk.com/open-source/inside-qiskit-ibms-open-source-quantum-computing-framework-3682891/) on 6 March 2019. Retrieved 11 December 2018.

6. Hemsoth, Nicole (August 7, 2018). "QISKit Developments Key to IBM Quantum Engagement" (https://www.nextplatform.com/2018/08/07/qiskit-developments-key-to-ibm-quantum-engagement/). *The Next Platform*. Archived (https://web.archive.org/web/20190306042859/https://www.nextplatform.com/2018/08/07/qiskit-developments-key-to-ibm-quantum-engagement/) from the original on 6 March 2019. Retrieved 11 December 2018.
7. "Qiskit Github page" (https://github.com/Qiskit). *GitHub*. Archived (https://web.archive.org/web/20210204053553/https://github.com/Qiskit) from the original on 2021-02-04. Retrieved 2018-11-05.
8. Wille, R.; Meter, R. Van; Naveh, Y. (March 25, 2019). "IBM's Qiskit Tool Chain: Working with and Developing for Real Quantum Computers". *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (https://ieeexplore.ieee.org/document/8715261). pp. 1234–1240. doi:10.23919/DATE.2019.8715261 (https://doi.org/10.23919%2FDATE.2019.8715261). ISBN 978-3-9819263-2-3. S2CID 155108078 (https://api.semanticscholar.org/CorpusID:155108078). Archived (https://web.archive.org/web/20221017103525/https://ieeexplore.ieee.org/document/8715261/) from the original on 2022-10-17. Retrieved 2023-12-30.
9. "Qiskit in swift" (https://github.com/Qiskit/qiskit-swift/). *GitHub*. Archived (https://web.archive.org/web/20211216230100/https://github.com/Qiskit/qiskit-swift/) from the original on December 16, 2021. Retrieved September 24, 2019.
10. "Qiskit (Quantum Information Science Kit) for JavaScript" (https://github.com/Qiskit/qiskit-js/). *GitHub*. Archived (https://web.archive.org/web/20180814153549/https://github.com/Qiskit/qiskit-js) from the original on August 14, 2018. Retrieved September 24, 2019.
11. "MicroQiskit" (https://github.com/qiskit-community/MicroQiskit). *GitHub*. Archived (https://web.archive.org/web/20220212051406/https://github.com/qiskit-community/MicroQiskit) from the original on February 12, 2022. Retrieved February 10, 2021.
12. "A collection of Jupyter notebooks showing how to use Qiskit that is synced with the IBM Quantum Experience" (https://github.com/Qiskit/qiskit-tutorial/). *GitHub*. Archived (https://web.archive.org/web/20180707052518/https://github.com/QISKit/qiskit-tutorial) from the original on July 7, 2018. Retrieved September 24, 2019.
13. "Celebrating the IBM Q Experience community, and their research" (https://www.ibm.com/blogs/research/2018/03/ibmq-published-research/). *IBM*. IBM Research Editorial Staff. March 8, 2018. Archived (https://web.archive.org/web/20191010224112/https://www.ibm.com/blogs/research/2018/03/ibmq-published-research/) from the original on October 10, 2019. Retrieved September 24, 2019.
14. "Learn Quantum Computing using Qiskit" (https://qiskit.org/textbook/preface.html). Archived (https://web.archive.org/web/20191220042259/https://qiskit.org/textbook/preface.html) from the original on 20 December 2019. Retrieved 20 December 2019.
15. Javadi-Abhari, Ali; Gambetta, Jay M. (July 13, 2018). "Qiskit and its Fundamental Elements" (https://medium.com/qiskit/qiskit-and-its-fundamental-elements-bcd7ead80492). *Medium*. Archived (https://web.archive.org/web/20190108055716/https://medium.com/qiskit/qiskit-and-its-fundamental-elements-bcd7ead80492) from the original on 8 January 2019. Retrieved 10 January 2019.
16. "Qiskit Terra" (https://web.archive.org/web/20191010224120/https://qiskit.org/Terra). *Qiskit*. Archived from the original (https://qiskit.org/Terra) on October 10, 2019. Retrieved September 24, 2019.
17. "An Open High-Performance Simulator for Quantum Circuits" (https://www.ibm.com/blogs/research/2018/05/quantum-circuits/). *IBM*. IBM Research Editorial Staff. May 1, 2018. Archived (https://web.archive.org/web/20190614124908/https://www.ibm.com/blogs/research/2018/05/quantum-circuits/) from the original on June 14, 2019. Retrieved September 24, 2019.

18. Wood, Christopher J. (December 19, 2018). "Introducing Qiskit Aer: A high performance simulator framework for quantum circuits" (https://medium.com/qiskit/qiskit-aer-d09d0fac7759). *Medium*. Archived (https://web.archive.org/web/20191101073346/https://medium.com/qiskit/qiskit-aer-d09d0fac7759) from the original on November 1, 2019. Retrieved September 24, 2019.
19. "IBM Q Experience community publishes research" (https://www.ibm.com/blogs/research/2018/03/ibmq-published-research/). *IBM Research Blog*. 2018-03-08. Archived (https://web.archive.org/web/20191010224112/https://www.ibm.com/blogs/research/2018/03/ibmq-published-research/) from the original on 2019-10-10. Retrieved 2021-07-14.
20. Wootton, James R.; Loss, Daniel (2018). "Repetition code of 15 qubits". *Physical Review A*. **97** (5): 052313. arXiv:1709.00990 (https://arxiv.org/abs/1709.00990). Bibcode:2018PhRvA..97e2313W (https://ui.adsabs.harvard.edu/abs/2018PhRvA..97e2313W). doi:10.1103/PhysRevA.97.052313 (https://doi.org/10.1103%2FPhysRevA.97.052313). ISSN 2469-9926 (https://search.worldcat.org/issn/2469-9926). S2CID 53444623 (https://api.semanticscholar.org/CorpusID:53444623).
21. Roffe, Joschka; Headley, David; Chancellor, Nicholas; Horsman, Dominic; Kendon, Viv (2018). "Protecting quantum memories using coherent parity check codes". *Quantum Science and Technology*. **3** (3): 035010. arXiv:1709.01866 (https://arxiv.org/abs/1709.01866). Bibcode:2018QS&T....3c5010R (https://ui.adsabs.harvard.edu/abs/2018QS&T....3c5010R). doi:10.1088/2058-9565/aac64e (https://doi.org/10.1088%2F2058-9565%2Faac64e). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 51684176 (https://api.semanticscholar.org/CorpusID:51684176).
22. Wang, Yuanhao; Li, Ying; Yin, Zhang-qi; Zeng, Bei (2018). "16-qubit IBM universal quantum computer can be fully entangled" (https://doi.org/10.1038%2Fs41534-018-0095-x). *npj Quantum Information*. **4** (1): 46. arXiv:1801.03782 (https://arxiv.org/abs/1801.03782). Bibcode:2018npjQI...4...46W (https://ui.adsabs.harvard.edu/abs/2018npjQI...4...46W). doi:10.1038/s41534-018-0095-x (https://doi.org/10.1038%2Fs41534-018-0095-x). ISSN 2056-6387 (https://search.worldcat.org/issn/2056-6387).
23. Zhukov, A. A.; Remizov, S. V.; Pogosov, W. V.; Lozovik, Yu. E. (2018). "Algorithmic simulation of far-from-equilibrium dynamics using quantum computer". *Quantum Information Processing*. **17** (9): 223. arXiv:1807.10149 (https://arxiv.org/abs/1807.10149). Bibcode:2018QuIP...17..223Z (https://ui.adsabs.harvard.edu/abs/2018QuIP...17..223Z). doi:10.1007/s11128-018-2002-y (https://doi.org/10.1007%2Fs11128-018-2002-y). ISSN 1570-0755 (https://search.worldcat.org/issn/1570-0755). S2CID 254991672 (https://api.semanticscholar.org/CorpusID:254991672).
24. *Qiskit/qiskit-ignis* (https://github.com/Qiskit/qiskit-ignis), Qiskit, archived (https://web.archive.org/web/20211221090311/https://github.com/Qiskit/qiskit-ignis) from the original on 2021-12-21, retrieved 2021-12-21.
25. "Ignis provides tools for quantum hardware verification, noise characterization, and error correction" (https://github.com/Qiskit/qiskit-ignis/). *GitHub*. Archived (https://web.archive.org/web/20190325181652/https://github.com/Qiskit/qiskit-ignis) from the original on March 25, 2019. Retrieved September 24, 2019.
26. "Qiskit Algorithms Migration Guide – Qiskit 0.28.0 documentation" (https://qiskit.org/documentation/aqua_tutorials/Qiskit%20Algorithms%20Migration%20Guide.html). *qiskit.org*. Archived (https://web.archive.org/web/20210714012130/https://qiskit.org/documentation/aqua_tutorials/Qiskit%20Algorithms%20Migration%20Guide.html) from the original on 2021-07-14. Retrieved 2021-07-14.
27. *Qiskit/qiskit-optimization* (https://github.com/Qiskit/qiskit-optimization), Qiskit, 2021-07-13, archived (https://web.archive.org/web/20220121053415/https://github.com/Qiskit/qiskit-optimization) from the original on 2022-01-21, retrieved 2021-07-14.
28. *Qiskit/qiskit-finance* (https://github.com/Qiskit/qiskit-finance), Qiskit, 2021-07-13, archived (https://web.archive.org/web/20211218120510/https://github.com/Qiskit/qiskit-finance) from the original on 2021-12-18, retrieved 2021-07-14.

29. *Qiskit/qiskit-machine-learning* (https://github.com/Qiskit/qiskit-machine-learning), Qiskit, 2021-07-13, archived (https://web.archive.org/web/20210722092257/https://github.com/Qiskit/qiskit-machine-learning) from the original on 2021-07-22, retrieved 2021-07-14.
30. *Qiskit/qiskit-nature* (https://github.com/Qiskit/qiskit-nature), Qiskit, 2021-07-13, archived (https://web.archive.org/web/20210816151130/https://github.com/Qiskit/qiskit-nature) from the original on 2021-08-16, retrieved 2021-07-14.

Further reading

- Qiskit Textbook (https://qiskit.org/learn/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Qiskit&oldid=1198321194"

WIKIPEDIA
The Free Encyclopedia

IBM Quantum Platform

IBM Quantum Platform (previously known as **IBM Quantum Experience**) is an online platform allowing public and premium access to cloud-based quantum computing services provided by IBM. This includes access to a set of IBM's prototype quantum processors, a set of tutorials on quantum computation, and access to an interactive textbook. As of February 2021, there are over 20 devices on the service, six of which are freely available for the public. This service can be used to run algorithms and experiments, and explore tutorials and simulations around what might be possible with quantum computing.

IBM Quantum Platform

IBM Quantum **Platform**	
Type of site	Cloud-based quantum computing
Owner	IBM
URL	quantum-computing.ibm.com (https://quantum-computing.ibm.com/)
Registration	Required
Launched	May 2016
Current status	Active

IBM's quantum processors are made up of superconducting transmon qubits, located in dilution refrigerators at the IBM Research headquarters at the Thomas J. Watson Research Center. Users interact with a quantum processor through the quantum circuit model of computation. Circuits can be created either graphically with the Quantum Composer, or programmatically with the Jupyter notebooks of the Quantum Lab. Circuits are created using Qiskit and can be compiled down to OpenQASM for execution on real quantum systems.

History

- The service was launched in May 2016 as the IBM Quantum Experience[1] with a five-qubit quantum processor and matching simulator connected in a star shaped pattern. At this time, users could only interact with the hardware through the quantum composer GUI. Quantum circuits were also limited to the specific two-qubit gates available on the hardware.
- In July 2016, IBM launched the IBM Quantum Experience community forum. This was subsequently replaced by a Slack workspace.
- In January 2017, IBM made a number of additions to the IBM Quantum Experience,[2] including increasing the set of two-qubit interactions available on the five-qubit quantum processor, expanding the simulator to custom topologies up to twenty qubits, and allowing users to interact with the device and simulator using quantum assembly language code.
- In March 2017, IBM released Qiskit[3] to enable users to more easily write code and run experiments on the quantum processor and simulator. A user guide for beginners was also added.
- In May 2017, IBM made an additional 16-qubit processor available on the IBM Quantum service.[4]

- In January 2018, IBM launched a quantum awards program, which it hosted on the IBM Quantum Experience.[5]
- In May 2019 a large overhaul of the service was made, including the addition of web-hosted Jupyter notebooks and integration with the online and interactive Qiskit textbook.[6]
- After a redesign in March 2021, a greater distinction was made between the composer GUI and the Jupyter notebooks. The *IBM Quantum Experience* name was retired in favour of the separate names *IBM Quantum Composer* and *IBM Quantum Lab*.[7] Now its collectively called *IBM Quantum Platform*.

IBM Quantum Composer

The Quantum Composer is a graphic user interface (GUI) designed by IBM to allow users to construct various quantum algorithms or run other quantum experiments. Users may see the results of their quantum algorithms by either running it on a real quantum processor or by using a simulator. Algorithms developed in the Quantum Composer are referred to as a "quantum score", in reference to the Quantum Composer resembling a musical sheet.[8]



Screenshot showing the result of running a GHZ state experiment using the IBM Quantum Composer

The composer can also be used in scripting mode, where the user can write programs in the OpenQASM-language instead. Below is an example of a very small program, built for IBMs 5-qubit computer. The program instructs the computer to generate a quantum state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, a 3-qubit GHZ state, which can be thought of as a variant of the Bell state, but with three qubits instead of two. It then measures the state, forcing it to collapse to one of the two possible outcomes, $|000\rangle$ or $|111\rangle$.

```
include "qelib1.inc"
qreg q[5];                // allocate 5 qubits (set automatically to |00000>)
creg c[5];                // allocate 5 classical bits

h q[0];                   // Hadamard-transform qubit 0
cx q[0], q[1];            // conditional pauli X-transform (ie. "CNOT") of qubits 0 and 1
                          // At this point we have a 2-qubit Bell state (|00> + |11>)/sqrt(2)

cx q[1], q[2];            // this expands entanglement to the 3rd qubit

measure q[0] -> c[0];     // this measurement collapses the entire 3-qubit state
measure q[1] -> c[1];     // therefore qubit 1 and 2 read the same value as qubit 0
measure q[2] -> c[2];
```

Every instruction in the QASM language is the application of a quantum gate, initialization of the chips registers to zero or measurement of these registers.

Usage

- In 2018 IBM reported that there were over 80,000 users of the IBM Quantum Experience, who have collectively run over 3 million experiments.[9]

- Many academic papers have been published by researchers who have conducted experiments using the service.[10][11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26][27]

References

1. "IBM Makes Quantum Computing Available on IBM Cloud to Accelerate Innovation" (https://web.archive.org/web/20160504214945/http://www-03.ibm.com/press/us/en/pressrelease/49661.wss). 2016-05-04. Archived from the original (https://www-03.ibm.com/press/us/en/pressrelease/49661.wss) on May 4, 2016.
2. "IBM Quantum Experience Update" (https://web.archive.org/web/20190129182024/https://quantumexperience.ng.bluemix.net/qstage/#/community/question?questionId=c7a17f4183104ea22ff8e3e8a95f794c). Archived from the original (https://quantumexperience.ng.bluemix.net/qstage/#/community/question?questionId=c7a17f4183104ea22ff8e3e8a95f794c) on 2019-01-29. Retrieved 2017-04-06.
3. "Quantum computing gets an API and SDK" (https://developer.ibm.com/dwblog/2017/quantum-computing-api-sdk-david-lubensky/). 2017-03-06.
4. "Beta access our upgrade to the IBM QX" (https://web.archive.org/web/20190131201233/https://quantumexperience.ng.bluemix.net/qx/community/question?questionId=db5f64ac99c6edc78e34932dfe593f36&channel=news). Archived from the original (https://quantumexperience.ng.bluemix.net/qx/community/question?questionId=db5f64ac99c6edc78e34932dfe593f36&channel=news) on 2019-01-31. Retrieved 2017-05-19.
5. "Now Open: Get quantum ready with new scientific prizes for professors, students and developers" (https://www.ibm.com/blogs/research/2018/01/quantum-prizes/). *IBM*. 2018-01-14.
6. "IBM Unveils Beta of Next Generation Quantum Development Platform" (https://www.ibm.com/blogs/research/2019/05/next-gen-ibmqx/). *IBM*. 2021-02-10.
7. "Announcement of IBM Quantum Composer and Lab" (https://twitter.com/jaygambetta/status/1366787131151163395). 2021-03-02.
8. "IBM Quantum experience" (https://web.archive.org/web/20180525063152/https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=59d2538efa783368715d988e06607b8c&pageIndex=0). *Quantum Experience*. IBM. Archived from the original (https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=59d2538efa783368715d988e06607b8c&pageIndex=0) on 25 May 2018. Retrieved 3 July 2017.
9. "IBM Collaborating With Top Startups to Accelerate Quantum Computing" (https://www.ibm.com/blogs/research/2018/04/ibm-startups-accelerate-quantum/). *IBM*. 2018-04-05.
10. "QX Community papers" (https://web.archive.org/web/20190322211226/https://quantumexperience.ng.bluemix.net/qx/community?channel=papers). Archived from the original (https://quantumexperience.ng.bluemix.net/qx/community?channel=papers) on 2019-03-22. Retrieved 2018-05-24.
11. "Research of the IBM Quantum Hub at the University of Melbourne" (https://www.unimelb.edu.au/quantumhub#research). 20 April 2021.
12. Rundle, R. P.; Tilma, T.; Samson, J. H.; Everitt, M. J. (2017). "Quantum state reconstruction made easy: a direct method for tomography". *Physical Review A*. **96** (2): 022117. arXiv:1605.08922 (https://arxiv.org/abs/1605.08922). Bibcode:2017PhRvA..96b2117R (https://ui.adsabs.harvard.edu/abs/2017PhRvA..96b2117R). doi:10.1103/PhysRevA.96.022117 (https://doi.org/10.1103%2FPhysRevA.96.022117).
13. Corbett Moran, Christine (29 June 2016). "Quintuple: a Python 5-qubit quantum computer simulator to facilitate cloud quantum computing". arXiv:1606.09225 (https://arxiv.org/abs/1606.09225) [quant-ph (https://arxiv.org/archive/quant-ph)].

14. Huffman, Emilie; Mizel, Ari (29 March 2017). "Violation of noninvasive macrorealism by a superconducting qubit: Implementation of a Leggett-Garg test that addresses the clumsiness loophole". *Physical Review A*. **95** (3): 032131. arXiv:1609.05957 (https://arxiv.org/abs/1609.05957). Bibcode:2017PhRvA..95c2131H (https://ui.adsabs.harvard.edu/abs/2017PhRvA..95c2131H). doi:10.1103/PhysRevA.95.032131 (https://doi.org/10.1103%2FPhysRevA.95.032131).
15. Deffner, Sebastian (23 September 2016). "Demonstration of entanglement assisted invariance on IBM's Quantum Experience" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5683883). *Heliyon*. **3** (11): e00444. arXiv:1609.07459 (https://arxiv.org/abs/1609.07459). doi:10.1016/j.heliyon.2017.e00444 (https://doi.org/10.1016%2Fj.heliyon.2017.e00444). PMC 5683883 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5683883). PMID 29159322 (https://pubmed.ncbi.nlm.nih.gov/29159322).
16. Huang, He-Liang; Zhao, You-Wei; Li, Tan; Li, Feng-Guang; Du, Yu-Tao; Fu, Xiang-Qun; Zhang, Shuo; Wang, Xiang; Bao, Wan-Su (9 December 2016). "Homomorphic Encryption Experiments on IBM's Cloud Quantum Computing Platform". *Frontiers of Physics*. **12** (1): 120305. arXiv:1612.02886 (https://arxiv.org/abs/1612.02886). Bibcode:2017FrPhy..12l0305H (https://ui.adsabs.harvard.edu/abs/2017FrPhy..12l0305H). doi:10.1007/s11467-016-0643-9 (https://doi.org/10.1007%2Fs11467-016-0643-9). S2CID 17770053 (https://api.semanticscholar.org/CorpusID:17770053).
17. Wootton, James R (1 March 2017). "Demonstrating non-Abelian braiding of surface code defects in a five qubit experiment". *Quantum Science and Technology*. **2** (1): 015006. arXiv:1609.07774 (https://arxiv.org/abs/1609.07774). Bibcode:2017QS&T....2a5006W (https://ui.adsabs.harvard.edu/abs/2017QS&T....2a5006W). doi:10.1088/2058-9565/aa5c73 (https://doi.org/10.1088%2F2058-9565%2Faa5c73). S2CID 44370109 (https://api.semanticscholar.org/CorpusID:44370109).
18. Fedortchenko, Serguei (8 July 2016). "A quantum teleportation experiment for undergraduate students". arXiv:1607.02398 (https://arxiv.org/abs/1607.02398) [quant-ph (https://arxiv.org/archive/quant-ph)].
19. Berta, Mario; Wehner, Stephanie; Wilde, Mark M (6 July 2016). "Entropic uncertainty and measurement reversibility". *New Journal of Physics*. **18** (7): 073004. arXiv:1511.00267 (https://arxiv.org/abs/1511.00267). Bibcode:2016NJPh...18g3004B (https://ui.adsabs.harvard.edu/abs/2016NJPh...18g3004B). doi:10.1088/1367-2630/18/7/073004 (https://doi.org/10.1088%2F1367-2630%2F18%2F7%2F073004). S2CID 119186679 (https://api.semanticscholar.org/CorpusID:119186679).
20. Li, Rui; Alvarez-Rodriguez, Unai; Lamata, Lucas; Solano, Enrique (23 November 2016). "Approximate Quantum Adders with Genetic Algorithms: An IBM Quantum Experience". *Quantum Measurements and Quantum Metrology*. **4** (1): 1–7. arXiv:1611.07851 (https://arxiv.org/abs/1611.07851). Bibcode:2017QMQM....4....1L (https://ui.adsabs.harvard.edu/abs/2017QMQM....4....1L). doi:10.1515/qmetro-2017-0001 (https://doi.org/10.1515%2Fqmetro-2017-0001). S2CID 108291239 (https://api.semanticscholar.org/CorpusID:108291239).
21. Hebenstreit, M.; Alsina, D.; Latorre, J. I.; Kraus, B. (11 January 2017). "Compressed quantum computation using the IBM Quantum Experience". *Phys. Rev. A*. **95** (5): 052339. arXiv:1701.02970 (https://arxiv.org/abs/1701.02970). doi:10.1103/PhysRevA.95.052339 (https://doi.org/10.1103%2FPhysRevA.95.052339). S2CID 118958024 (https://api.semanticscholar.org/CorpusID:118958024).
22. Alsina, Daniel; Latorre, José Ignacio (11 July 2016). "Experimental test of Mermin inequalities on a five-qubit quantum computer". *Physical Review A*. **94** (1): 012314. arXiv:1605.04220 (https://arxiv.org/abs/1605.04220). Bibcode:2016PhRvA..94a2314A (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94a2314A). doi:10.1103/PhysRevA.94.012314 (https://doi.org/10.1103%2FPhysRevA.94.012314). S2CID 119189277 (https://api.semanticscholar.org/CorpusID:119189277).

23. Linke, Norbert M.; Maslov, Dmitri; Roetteler, Martin; Debnath, Shantanu; Figgatt, Caroline; Landsman, Kevin A.; Wright, Kenneth; Monroe, Christopher (28 March 2017). "Experimental comparison of two quantum computing architectures" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5380037). *Proceedings of the National Academy of Sciences*. **114** (13): 3305–3310. arXiv:1702.01852 (https://arxiv.org/abs/1702.01852). Bibcode:2017PNAS..114.3305L (https://ui.adsabs.harvard.edu/abs/2017PNAS..114.3305L). doi:10.1073/pnas.1618020114 (https://doi.org/10.1073%2Fpnas.1618020114). PMC 5380037 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5380037). PMID 28325879 (https://pubmed.ncbi.nlm.nih.gov/28325879).
24. Devitt, Simon J. (29 September 2016). "Performing quantum computing experiments in the cloud". *Physical Review A*. **94** (3): 032329. arXiv:1605.05709 (https://arxiv.org/abs/1605.05709). Bibcode:2016PhRvA..94c2329D (https://ui.adsabs.harvard.edu/abs/2016PhRvA..94c2329D). doi:10.1103/PhysRevA.94.032329 (https://doi.org/10.1103%2FPhysRevA.94.032329). S2CID 119217150 (https://api.semanticscholar.org/CorpusID:119217150).
25. Steiger, Damian; Haner, Thomas; Troyer, Matthias (2018). "ProjectQ: An Open Source Software Framework for Quantum Computing". *Quantum*. **2**: 49. arXiv:1612.08091 (https://arxiv.org/abs/1612.08091). Bibcode:2018Quant...2...49S (https://ui.adsabs.harvard.edu/abs/2018Quant...2...49S). doi:10.22331/q-2018-01-31-49 (https://doi.org/10.22331%2Fq-2018-01-31-49). S2CID 6758479 (https://api.semanticscholar.org/CorpusID:6758479).
26. Santos, Alan C. (2017). "O Computador Quântico da IBM e o IBM Quantum Experience". *Revista Brasileira de Ensino de Física*. **39** (1). arXiv:1610.06980 (https://arxiv.org/abs/1610.06980). doi:10.1590/1806-9126-RBEF-2016-0155 (https://doi.org/10.1590%2F1806-9126-RBEF-2016-0155).
27. Caicedo-Ortiz, H. E.; Santiago-Cortés, E. (2017). "Construyendo compuertas cuánticas con IBM's cloud quantum computer" (http://jci.uniautonoma.edu.co/2017/2017-7.pdf) [Building quantum gates with IBM's cloud quantum computer] (PDF). *Journal de Ciencia e Ingeniería* (in Spanish). **9**: 42–56. doi:10.46571/JCI.2017.1.7 (https://doi.org/10.46571%2FJCI.2017.1.7).

External links

- IBM Quantum Platform (https://quantum-computing.ibm.com/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=IBM_Quantum_Platform&oldid=1242250815"

WIKIPEDIA
The Free Encyclopedia

Quil (instruction set architecture)

Quil is a quantum instruction set architecture that first introduced a shared quantum/classical memory model. It was introduced by Robert Smith, Michael Curtis, and William Zeng in *A Practical Quantum Instruction Set Architecture*.[1] Many quantum algorithms (including quantum teleportation, quantum error correction, simulation,[2][3] and optimization algorithms[4]) require a shared memory architecture. Quil is being developed for the superconducting quantum processors developed by Rigetti Computing through the Forest quantum programming API.[5][6] A Python library called `pyQuil` was introduced to develop Quil programs with higher level constructs. A Quil backend is also supported by other quantum programming environments.[7][8]

Underlying quantum abstract machine

In the paper presented by Smith, Curtis and Zeng, Quil specifies the instruction set for a Quantum Abstract Machine (QAM,) akin to a Turing machine, yet more practical for accomplishing "real-world" tasks.[1] The state of the QAM can be represented as a 6-tuple $(|\Psi\rangle, C, G, G', P, \kappa)$ where:

- $|\Psi\rangle$ is the (quantum) state of a fixed but arbitrary number of qubits N_q indexed using a 0-based indexing.
- C is a classical memory of a number N_c of classical bits indexed using a 0-based indexing.
- G a fixed but arbitrary list of static gates (quantum gates that do not depend on parameters, like the Hadamard gate.)
- G' a fixed but arbitrary list of parametric gates (gates that depend on a number of complex parameters like the phase shift gate that requires an angle parameter to be completely defined.)
- P a sequence of Quil instructions to be executed, representing the program. The length of P is denoted by $|P|$.
- κ an integer program counter pointing to the next instruction to be executed. κ always starts at 0 (pointing to the 0^{th} instruction) and ends at $|P|$ indicating program halting (note that the last instruction has the index $|P| - 1$.) The program counter is incremented after every instruction, except for special control flow instructions (conditional and unconditional jumps, and the special `HALT` instruction that halts the program by setting κ to $|P|$.

The semantics of the QAM are defined using tensor products of Hilbert spaces and the linear maps between them.[1]

Features

Quil has support for defining possibly parametrized gates in matrix form (the language does not include a way to verify that the matrices are unitary, which is a necessary condition for the physical realizability of the defined gate) and their application on qubits. The language also supports macro-like definitions of possibly parametrized quantum circuits and their expansion, qubit measurement and recording of the outcome in classical memory, synchronization with classical computers with the `WAIT` instruction which

pauses the execution of a Quil program until a classical program has ended its execution, conditional and unconditional branching, pragma support, as well as inclusion of files for use as libraries (a standard set of gates is provided as one of the libraries.)

Rigetti QVM

Rigetti Computing developed a quantum virtual machine in Common Lisp that simulates the defined Quantum Abstract Machine on a classical computer and is capable of the parsing and execution of Quil programs with possibly remote execution via HTTP.[9]

Example

The following example demonstrates the classical control flow needed to do quantum teleportation of the qubit in register 2 to register 1:[10][11]

```
# Declare classical memory
DECLARE ro BIT[2]
# Create Bell Pair
H 0
CNOT 0 1
# Teleport
CNOT 2 0
H 2
MEASURE 2 ro[0]
MEASURE 0 ro[1]
# Classically communicate measurements
JUMP-UNLESS @SKIP ro[1]
X 1
LABEL @SKIP
JUMP-UNLESS @END ro[0]
Z 1
LABEL @END
```

Examples of the implementations of the quantum fourier transform and the variational quantum Eigensolver are given in the paper.

References

1. Smith, Robert S.; Curtis, Michael J.; Zeng, William J. (2016-08-10). "A Practical Quantum Instruction Set Architecture". arXiv:1608.03355 (https://arxiv.org/abs/1608.03355) [quant-ph (https://arxiv.org/archive/quant-ph)].
2. McClean, Jarrod R.; Romero, Jonathan; Babbush, Ryan; Aspuru-Guzik, Alán (2016-02-04). "The theory of variational hybrid quantum-classical algorithms". *New Journal of Physics*. **18** (2): 023023. arXiv:1509.04279 (https://arxiv.org/abs/1509.04279). Bibcode:2016NJPh...18b3023M (https://ui.adsabs.harvard.edu/abs/2016NJPh...18b3023M). doi:10.1088/1367-2630/18/2/023023 (https://doi.org/10.1088%2F1367-2630%2F18%2F2%2F023023). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 92988541 (https://api.semanticscholar.org/CorpusID:92988541).
3. Rubin, Nicholas C. (2016-10-21). "A Hybrid Classical/Quantum Approach for Large-Scale Studies of Quantum Systems with Density Matrix Embedding Theory". arXiv:1610.06910 (https://arxiv.org/abs/1610.06910) [quant-ph (https://arxiv.org/archive/quant-ph)].

4. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014-11-14). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
5. "Rigetti Launches Full-Stack Quantum Computing Service and Quantum IC Fab" (https://spectrum.ieee.org/rigetti-launches-fullstack-quantum-computing-service-and-quantum-ic-fab). *IEEE Spectrum: Technology, Engineering, and Science News*. 26 June 2017. Retrieved 2017-07-06.
6. "Rigetti Quietly Releases Beta of Forest Platform for Quantum Programming in the Cloud | Quantum Computing Report" (https://quantumcomputingreport.com/news/rigetti-quietly-releases-beta-of-forest-platform-for-quantum-programming-in-the-cloud/). *quantumcomputingreport.com*. 8 March 2017. Retrieved 2017-07-06.
7. "XACC Rigetti Accelerator" (https://ornl-qci.github.io/xacc/accelerators/rigetti). *ornl-qci.github.io*. Retrieved 2017-07-06.
8. Doiron, Nick (2017-03-07), *jsquil: Quantum computer instructions for JavaScript developers* (https://github.com/mapmeld/jsquil), retrieved 2017-07-06
9. *The @rigetti high-performance quantum virtual machine.: rigetti/qvm* (https://github.com/rigetti/qvm), Rigetti Computing, 2019-04-26, retrieved 2019-04-28
10. Nielsen, Michael A.; Chuang, Isaac L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press. p. 27. ISBN 978-0-521-63503-5.
11. Computing, Rigetti (28 May 2019). "pyQuil Documentation" (https://media.readthedocs.org/pdf/pyquil/latest/pyquil.pdf) (PDF). *pyQuil Documentaion*. Retrieved 6 June 2019.

External links

- quil (https://github.com/quil-lang/quil) on GitHub GitHub repository

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quil_(instruction_set_architecture)&oldid=1237719911"

WIKIPEDIA
The Free Encyclopedia

Rigetti Computing

Rigetti Computing, Inc. is a Berkeley, California-based developer of quantum integrated circuits used for quantum computers. The company also develops a cloud platform called Forest that enables programmers to write quantum algorithms.[2]

Rigetti Computing, Inc.

Company type	Public
Traded as	Nasdaq: RGTI (https://www.nasdaq.com/market-activity/stocks/rgti)
Industry	Quantum computing
Founded	2013
Founder	Chad Rigetti
Headquarters	Berkeley, California, United States
Key people	Subodh Kulkarni (CEO)
Products	Quantum integrated circuits Forest quantum computing software
Revenue	▼ US$12 million (2023)
Number of employees	134 (2024)
Website	rigetti.com (http://rigetti.com)

Footnotes / references
[1]

History

Traces of Rigetti Computing can be dated back to 1980, however the company was officially founded in 2013.

Rigetti Computing was founded in 2013 by Chad Rigetti, a physicist who previously worked on quantum computers at IBM, and studied under Michel Devoret.[2][3] The company emerged from startup incubator Y Combinator in 2014 as a so-called "spaceshot" company.[4][5] The company also went through enterprise revenue-focused The Alchemist Accelerator in 2014.[5]

By February 2016, the company had begun testing a three-qubit (quantum bit) chip made using aluminum circuits on a silicon wafer.[6] In March, the company raised Series A funding of US$24 million in a round led by Andreessen Horowitz. In November, the company raised Series B funding of $40 million in a round led by investment firm Vy Capital, along with additional funding from Andreessen Horowitz and other investors. Y Combinator was a smaller investor in both rounds.[5]

By Spring of 2017, the company was testing eight-qubit computers,[3] and in June, the company announced the public beta availability of a quantum cloud computing platform called Forest 1.0, which allows developers to write quantum algorithms.[2]

In October 2021, it was announced that the company planned to go public via a SPAC merger, with estimated valuation around $1.5 billion.[7][8] This process was expected to raise an addition $458 million in funding, in addition to the $200 million raised previously.[7] With this funding, Rigetti planned to scale its systems from 80 qubits to 1,000 qubits by 2024, and to 4,000 by 2026.[9] The SPAC deal closed on 2 March 2022, and the company shares began trading on the NASDAQ exchange.[10]

In December 2022, Subodh Kulkarni became president and CEO of the company.[11]

In July 2023 Rigetti launched a single chip 84 qubit quantum processor that can scale to larger systems.[12]

Products and technology

Rigetti Computing is a full-stack quantum computing company, a term that indicates that the company designs and fabricates quantum chips, integrates them with a controlling architecture, and develops software for programmers to use to build algorithms for the chips.[13]

Forest cloud computing platform

The company hosts a cloud computing platform called Forest, which gives developers access to quantum processors so they can write quantum algorithms for testing purposes. The computing platform is based on a custom instruction language the company developed called Quil, which stands for Quantum Instruction Language. Quil facilitates hybrid quantum/classical computing, and programs can be built and executed using open source Python tools.[13][14] As of June 2017, the platform allows coders to write quantum algorithms for a simulation of a quantum chip with 36 qubits.[2]

Fab-1

The company operates a rapid prototyping fabrication ("fab") lab called Fab-1, designed to quickly create integrated circuits. Lab engineers design and generate experimental designs for 3D-integrated quantum circuits for qubit-based quantum hardware.[13]

Recognition

The company was recognized in 2016 by X-Prize founder Peter Diamandis as being one of the three leaders in the quantum computing space, along with IBM and Google.[15] MIT Technology Review named the company one of the 50 smartest companies of 2017.[16]

See also

- D-Wave Systems
- Quantum Computing Inc. (http://www.quantumcomputinginc.com)

Locations

Rigetti Computing is headquartered in Berkeley, California, where it hosts developmental systems and cooling equipment.[15] The company also operates its Fab-1 manufacturing facility in nearby Fremont.[2]

References

1. "Rigetti Computing Inc. 2023 Annual Report (Form 10-K)" (https://www.sec.gov/ix?doc=/Arc

hives/edgar/data/1838359/000155837024003234/tmb-20231231x10k.htm). U.S. Securities and Exchange Commission. March 14, 2024.
2. "The Quantum Computer Factory That's Taking on Google and IBM" (https://www.wired.com/story/quantum-computing-factory-taking-on-google-ibm/). *wired.com*. 2017-06-20. Retrieved 2017-07-20.
3. "A quantum leap of faith" (https://www.uregina.ca/external/communications/assets/docs/pdf/degrees-magazine/dm-ss2017.pdf#page=22) (PDF). *uregina.com*. 2017-06-20. Retrieved 2017-07-20.
4. "11 startups to watch from Y Combinator's Demo Day" (http://www.bizjournals.com/sanjose/news/2014/08/20/11-startups-to-watch-from-y-combinators-demo-day.html). *bizjournals.com*. Silicon Valley Business Journal. 2014-08-20. Retrieved 2017-07-20.
5. "Y Combinator's quantum computing 'spaceshot' scores $64M from A16Z, others" (http://www.bizjournals.com/sanjose/news/2017/03/28/rigetti-quantum-computing-y-combinator-a16z.html). *bizjournals.com*. Silicon Valley Business Journal. 2017-03-29. Retrieved 2017-07-20.
6. "The Tiny Startup Racing Google to Build a Quantum Computing Chip" (https://www.technologyreview.com/s/600711/the-tiny-startup-racing-google-to-build-a-quantum-computing-chip/). *technologyreview.com*. 2016-02-08. Retrieved 2017-07-20.
7. "Rigetti Announces SPAC Deal with Supernova II" (https://www.rigetti.com/merger-announcement). *Rigetti*. Retrieved 2021-10-11.
8. Lee, Jane Lanhee (2021-10-06). "Quantum computer maker Rigetti to go public via $1.5 bln SPAC deal" (https://www.reuters.com/technology/quantum-computer-maker-rigetti-go-public-via-15-bln-spac-deal-2021-10-06/). *Reuters*. Retrieved 2021-10-11.
9. "Quantum-Computing Company Rigetti to Go Public Through SPAC Deal" (https://www.marketwatch.com/story/quantum-computing-company-rigetti-to-go-public-through-spac-deal-271633523304). *MarketWatch*. Retrieved 2021-10-11.
10. "Rigetti Computing Announces Closing of Business Combination with Supernova Partners Acquisition Company II, Ltd.; Begins Trading on Nasdaq Capital Market Today" (https://www.globenewswire.com/news-release/2022/03/02/2395179/0/en/Rigetti-Computing-Announces-Closing-of-Business-Combination-with-Supernova-Partners-Acquisition-Company-II-Ltd-Begins-Trading-on-Nasdaq-Capital-Market-Today.html). *globenewswire.com* (Press release). 2 March 2022.
11. "Dr. Subodh Kulkarni | Rigetti Computing" (https://www.rigetti.com/leadership-team/dr-subodh-kulkarni). *Rigetti*. Retrieved 2023-07-11.
12. "Rigetti launches 84qubit single chip quantum processor" (https://www.eenewseurope.com/en/rigetti-launches-84qubit-single-chip-quantum-processor/). August 11, 2023.
13. "Rigetti Launches Full-Stack Quantum Computing Service and Quantum IC Fab" (https://spectrum.ieee.org/rigetti-launches-fullstack-quantum-computing-service-and-quantum-ic-fab). *IEEE*. 2017-06-26. Retrieved 2017-07-20.
14. "Welcome to pyQuil!" (https://pyquil.readthedocs.io). *readthedocs.io*. Retrieved 2017-07-20.
15. Md, Peter H. Diamandis (2010-10-16). "Massive Disruption Is Coming With Quantum Computing" (https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/). *Singularity Hub*. Retrieved 2017-07-20.
16. "50 Smartest Companies 2017" (https://www.technologyreview.com/lists/companies/2017/#rigetti-computing). *technologyreview.com*. Retrieved 2017-07-20.

External links

- Official website (https://www.rigetti.com)
- Business data for Rigetti Computing: Bloomberg (https://www.bloomberg.com/quote/RGTI:US) · Google (https://www.google.com/finance/quote/RGTI) · SEC filings (https://www.sec.go

v/cgi-bin/browse-edgar?action=getcompany&CIK=1838359) · Yahoo! (https://finance.yahoo.com/quote/RGTI)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Rigetti_Computing&oldid=1237720748"

WIKIPEDIA
The Free Encyclopedia

Cirq

Cirq is an open-source framework for noisy intermediate scale quantum (NISQ) computers.[1]

Cirq	
Developers	quantumlib (https://github.com/quantumlib)
Implementation language	Python
License	Apache license (https://github.com/quantumlib/Cirq/blob/master/LICENSE)
Website	GitHub (https://github.com/quantumlib/Cirq)

History

Cirq was developed by the Google AI Quantum Team, and the public alpha was announced at the International Workshop on Quantum Software and Quantum Machine Learning on July 18, 2018.[2] A demo by QC Ware showed an implementation of QAOA solving an example of the maximum cut problem being solved on a Cirq simulator.[3]

Usage

Quantum programs in Cirq are represented by "Circuit" which is made up of a series of "Moments" representing slices of quantum gates that should be applied at the same time.[4] The programs can be executed on local simulators[5] or against hardware supplied by IonQ, Pasqal,[6] Rigetti, and Alpine Quantum Technologies[7]

The following example shows how to create and measure a Bell state in Cirq.

```
import cirq

# Pick qubits
qubit0 = cirq.GridQubit(0, 0)
qubit1 = cirq.GridQubit(0, 1)

# Create a circuit
circuit = cirq.Circuit.from_ops(
    cirq.H(qubit0),
    cirq.CNOT(qubit0, qubit1),
    cirq.measure(qubit0, key="m0"),
    cirq.measure(qubit1, key="m1")
)
```

Printing the circuit displays its diagram

```
print(circuit)
# prints
# (0, 0): ———H———@———M('m0')———
#                 |
# (0, 1): ———————X———M('m1')———
```

Simulating the circuit repeatedly shows that the measurements of the qubits are correlated.

```
simulator = cirq.Simulator()
result = simulator.run(circuit, repetitions=5)
print(result)
# prints
# m0=11010
# m1=11010
```

Projects

OpenFermion

OpenFermion is a library that compiles quantum simulation algorithms to Cirq.[2]

TensorFlow Quantum

TensorFlow Quantum is an extension of TensorFlow that allows TensorFlow to be used to explore hybrid classical-quantum machine learning algorithms.[8]

ReCirq

ReCirq is a repository of research projects done using Cirq.[9]

Qsim Cirq

Qsim is a high performance wave function simulator that leverages gate fusing, AVS/FMA instructions, and OpenMP to achieve fast simulation rates. Qsimcirq allows one to use qsim from within Cirq.[10]

References

1. Fingerhuth, Mark; Babej, Tomáš; Wittek, Peter (2018). "Open source software in quantum computing" (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6301779). *PLOS ONE*. **13** (12): e0208561. arXiv:1812.09167 (https://arxiv.org/abs/1812.09167). Bibcode:2018PLoSO..1308561F (https://ui.adsabs.harvard.edu/abs/2018PLoSO..1308561F). doi:10.1371/journal.pone.0208561 (https://doi.org/10.1371%2Fjournal.pone.0208561). PMC 6301779 (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6301779). PMID 30571700 (https://pubmed.ncbi.nlm.nih.gov/30571700).
2. Ho, Alan; Bacon, Dave (2018-07-18). "Announcing Cirq: An Open Source Framework for NISQ Algorithms" (https://ai.googleblog.com/2018/07/announcing-cirq-open-source-framework.html). *Google AI Blog*. Google AI Quantum Team. Retrieved 2019-03-06.
3. "public_demos/max_cut_cirq.py at master · qcware/public_demos · GitHub" (https://web.archive.org/web/20180720153354/https://github.com/qcware/public_demos/blob/master/max_cut/max_cut_cirq.py). *GitHub*. 20 July 2018. Archived from the original (https://github.com/qcware/public_demos/blob/master/max_cut/max_cut_cirq.py) on 20 July 2018. Retrieved 29 October 2019.
4. "Cirq Circuits" (https://quantumai.google/cirq/start/basics#circuits_and_moments). *Google Quantum AI website*. Google AI Quantum Team. Retrieved 2022-07-06.
5. "Cirq Simulation" (https://quantumai.google/cirq/simulate). *Google Quantum AI website*. Retrieved 2022-07-06.

6. "Pasqal" (https://pasqal.io/).
7. "AQT" (https://www.aqt.eu/).
8. "TensorFlow Quantum" (https://www.tensorflow.org/quantum). *TensorFlow*. Retrieved 2022-07-06.
9. "ReCirq" (https://github.com/quantumlib/ReCirq). *Google Quantum Github*. Retrieved 2022-07-06.
10. "qsimcirq" (https://pypi.org/project/qsimcirq/). Retrieved 2022-07-06.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Cirq&oldid=1213672645"

WIKIPEDIA
The Free Encyclopedia

Q Sharp

Q# (pronounced as *Q sharp*) is a domain-specific programming language used for expressing quantum algorithms.[3] It was initially released to the public by Microsoft as part of the Quantum Development Kit.[4]

Q# works in conjunction with classical languages such as C#, Python and F#, and is designed to allow the use of traditional programming concepts in quantum computing, including functions with variables and branches as well as a syntax-highlighted development environment with a quantum debugger.[1][5][6]

Q#

Paradigm	Quantum, functional, imperative
Designed by	Microsoft Research (quantum architectures and computation group; QuArC)
Developer	Microsoft
First appeared	December 11, 2017[1]
Typing discipline	Static, strong
Platform	Common Language Infrastructure
License	MIT License[2]
Filename extensions	.qs
Website	docs.microsoft.com/en-us/quantum (https://docs.microsoft.com/en-us/quantum)
Influenced by	
C#, F#, Python	

History

Historically, Microsoft Research had two teams interested in quantum computing: the QuArC team based in Redmond, Washington,[7] directed by Krysta Svore, that explored the construction of quantum circuitry, and Station Q initially located in Santa Barbara and directed by Michael Freedman, that explored topological quantum computing.[8][9]

During a Microsoft Ignite Keynote on September 26, 2017, Microsoft announced that they were going to release a new programming language geared specifically towards quantum computers.[10] On December 11, 2017, Microsoft released Q# as a part of the Quantum Development Kit.[4]

At Build 2019, Microsoft announced that it would be open-sourcing the Quantum Development Kit, including its Q# compilers and simulators.[11]

To support Q#, Microsoft developed Quantum Intermediate Representation (QIR) in 2023 as a common interface between programming languages and target quantum processors. The company also announced a compiler extension that generates QIR from Q#.[12]

Bettina Heim currently leads the Q# language development effort.[13][14]

Usage

Q# is available as a separately downloaded extension for Visual Studio,[15] but it can also be run as an independent tool from the command line or Visual Studio Code. Q# was introduced on Windows and is available on MacOS and Linux.[16]

The Quantum Development Kit includes a quantum simulator capable of running Q# and simulated 30 logical qubits.[17][18]

In order to invoke the quantum simulator, another .NET programming language, usually C#, is used, which provides the (classical) input data for the simulator and reads the (classical) output data from the simulator.[19]

Features

A primary feature of Q# is the ability to create and use qubits for algorithms. As a consequence, some of the most prominent features of Q# are the ability to entangle and introduce superpositioning to qubits via Controlled NOT gates and Hadamard gates, respectively, as well as Toffoli Gates, Pauli X, Y, Z Gate, and many more which are used for a variety of operations; see the list at the article on quantum logic gates.[20]

The hardware stack that will eventually come together with Q# is expected to implement Qubits as topological qubits. The quantum simulator that is shipped with the Quantum Development Kit today is capable of processing up to 32 qubits on a user machine and up to 40 qubits on Azure.[21]

Documentation and resources

Currently, the resources available for Q# are scarce, but the official documentation is published: Microsoft Developer Network: Q# (https://docs.microsoft.com/en-us/quantum/?view=qsharp-preview). Microsoft Quantum Github repository (https://github.com/Microsoft/Quantum/) is also a large collection of sample programs implementing a variety of Quantum algorithms and their tests.

Microsoft has also hosted a Quantum Coding contest on Codeforces, called Microsoft Q# Coding Contest - Codeforces (https://web.archive.org/web/20181119064628/https://codeforces.com/msqs2018), and also provided related material to help answer the questions in the blog posts, plus the detailed solutions in the tutorials.

Microsoft hosts a set of learning exercises to help learn Q# on GitHub: microsoft/QuantumKatas (https://github.com/Microsoft/QuantumKatas) with links to resources, and answers to the problems.

Syntax

Q# is syntactically related to both C# and F# yet also has some significant differences.

Similarities with C#

- Uses `namespace` for code isolation
- All statements end with a `;`
- Curly braces are used for statements of scope
- Single line comments are done using `//`

- Variable data types such as `Int` `Double` `String` and `Bool` are similar, although capitalised (and Int is 64-bit)[22]
- Qubits are allocated and disposed inside a `using` block.
- Lambda functions are defined using the => operator.
- Results are returned using the `return` keyword.

Similarities with F#

- Variables are declared using either `let` or `mutable`[3]
- First-order functions
- Modules, which are imported using the `open` keyword
- The datatype is declared after the variable name
- The range operator `..`
- `for … in` loops
- Every operation/function has a return value, rather than `void`. Instead of `void`, an empty Tuple `()` is returned.
- Definition of record datatypes (using the `newtype` keyword, instead of `type`).

Differences

- Functions are declared using the `function` keyword
- Operations on the quantum computer are declared using the `operation` keyword
- Lack of multiline comments
- Asserts instead of throwing exceptions
- Documentation is written in Markdown instead of XML-based documentation tags

Example

The following source code is a multiplexer from the official Microsoft Q# library repository.

```
// Copyright (c) Microsoft Corporation.
// Licensed under the MIT License.

namespace Microsoft.Quantum.Canon {
    open Microsoft.Quantum.Intrinsic;
    open Microsoft.Quantum.Arithmetic;
    open Microsoft.Quantum.Arrays;
    open Microsoft.Quantum.Diagnostics;
    open Microsoft.Quantum.Math;

    /// # Summary
    /// Applies a multiply-controlled unitary operation $U$ that applies a
    /// unitary $V_j$ when controlled by n-qubit number state $\ket{j}$.
    ///
    /// $U = \sum^{N-1}_{j=0}\ket{j}\bra{j}\otimes V_j$.
    ///
    /// # Input
    /// ## unitaryGenerator
    /// A tuple where the first element `Int` is the number of unitaries $N$,
    /// and the second element `(Int -> ('T => () is Adj + Ctl))`
    /// is a function that takes an integer $j$ in $[0,N-1]$ and outputs the unitary
```

```
    /// operation $V_j$.
    ///
    /// ## index
    /// $n$-qubit control register that encodes number states $\ket{j}$ in
    /// little-endian format.
    ///
    /// ## target
    /// Generic qubit register that $V_j$ acts on.
    ///
    /// # Remarks
    /// `coefficients` will be padded with identity elements if
    /// fewer than $2^n$ are specified. This implementation uses
    /// $n-1$ auxiliary qubits.
    ///
    /// # References
    /// - [ *Andrew M. Childs, Dmitri Maslov, Yunseong Nam, Neil J. Ross, Yuan Su*,
    ///      arXiv:1711.10980](https://arxiv.org/abs/1711.10980)
    operation MultiplexOperationsFromGenerator<'T>(unitaryGenerator : (Int, (Int -> ('T => Unit is Adj
+ Ctl))), index: LittleEndian, target: 'T) : Unit is Ctl + Adj {
        let (nUnitaries, unitaryFunction) = unitaryGenerator;
        let unitaryGeneratorWithOffset = (nUnitaries, 0, unitaryFunction);
        if Length(index!) == 0 {
            fail "MultiplexOperations failed. Number of index qubits must be greater than 0.";
        }
        if nUnitaries > 0 {
            let auxiliary = [];
            Adjoint MultiplexOperationsFromGeneratorImpl(unitaryGeneratorWithOffset, auxiliary, index,
target);
        }
    }

    /// # Summary
    /// Implementation step of `MultiplexOperationsFromGenerator`.
    /// # See Also
    /// - Microsoft.Quantum.Canon.MultiplexOperationsFromGenerator
    internal operation MultiplexOperationsFromGeneratorImpl<'T>(unitaryGenerator : (Int, Int, (Int ->
('T => Unit is Adj + Ctl))), auxiliary: Qubit[], index: LittleEndian, target: 'T)
    : Unit {
        body (...) {
            let nIndex = Length(index!);
            let nStates = 2^nIndex;

            let (nUnitaries, unitaryOffset, unitaryFunction) = unitaryGenerator;

            let nUnitariesLeft = MinI(nUnitaries, nStates / 2);
            let nUnitariesRight = MinI(nUnitaries, nStates);

            let leftUnitaries = (nUnitariesLeft, unitaryOffset, unitaryFunction);
            let rightUnitaries = (nUnitariesRight - nUnitariesLeft, unitaryOffset + nUnitariesLeft,
unitaryFunction);

            let newControls = LittleEndian(Most(index!));

            if nUnitaries > 0 {
                if Length(auxiliary) == 1 and nIndex == 0 {
                    // Termination case

                    (Controlled Adjoint (unitaryFunction(unitaryOffset)))(auxiliary, target);
                } elif Length(auxiliary) == 0 and nIndex >= 1 {
                    // Start case
                    let newauxiliary = Tail(index!);
                    if nUnitariesRight > 0 {
                        MultiplexOperationsFromGeneratorImpl(rightUnitaries, [newauxiliary],
newControls, target);
                    }
                    within {
                        X(newauxiliary);
                    } apply {
                        MultiplexOperationsFromGeneratorImpl(leftUnitaries, [newauxiliary],
newControls, target);
                    }
                } else {
                    // Recursion that reduces nIndex by 1 and sets Length(auxiliary) to 1.
                    let controls = [Tail(index!)] + auxiliary;
                    use newauxiliary = Qubit();
```

```
                    use andauxiliary = Qubit[MaxI(0, Length(controls) - 2)];
                    within {
                        ApplyAndChain(andauxiliary, controls, newauxiliary);
                    } apply {
                        if nUnitariesRight > 0 {
                            MultiplexOperationsFromGeneratorImpl(rightUnitaries, [newauxiliary],
newControls, target);
                        }
                        within {
                            (Controlled X)(auxiliary, newauxiliary);
                        } apply {
                            MultiplexOperationsFromGeneratorImpl(leftUnitaries, [newauxiliary],
newControls, target);
                        }
                    }
                }
            }
        }
        adjoint auto;
        controlled (controlRegister, ...) {
            MultiplexOperationsFromGeneratorImpl(unitaryGenerator, auxiliary + controlRegister, index,
target);
        }
        adjoint controlled auto;
    }

    /// # Summary
    /// Applies multiply-controlled unitary operation $U$ that applies a
    /// unitary $V_j$ when controlled by n-qubit number state $\ket{j}$.
    ///
    /// $U = \sum^{N-1}_{j=0}\ket{j}\bra{j}\otimes V_j$.
    ///
    /// # Input
    /// ## unitaryGenerator
    /// A tuple where the first element `Int` is the number of unitaries $N$,
    /// and the second element `(Int -> ('T => () is Adj + Ctl))`
    /// is a function that takes an integer $j$ in $[0,N-1]$ and outputs the unitary
    /// operation $V_j$.
    ///
    /// ## index
    /// $n$-qubit control register that encodes number states $\ket{j}$ in
    /// little-endian format.
    ///
    /// ## target
    /// Generic qubit register that $V_j$ acts on.
    ///
    /// # Remarks
    /// `coefficients` will be padded with identity elements if
    /// fewer than $2^n$ are specified. This version is implemented
    /// directly by looping through n-controlled unitary operators.
    operation MultiplexOperationsBruteForceFromGenerator<'T>(unitaryGenerator : (Int, (Int -> ('T =>
Unit is Adj + Ctl))), index: LittleEndian, target: 'T)
    : Unit is Adj + Ctl {
        let nIndex = Length(index!);
        let nStates = 2^nIndex;
        let (nUnitaries, unitaryFunction) = unitaryGenerator;
        for idxOp in 0..MinI(nStates,nUnitaries) - 1 {
            (ControlledOnInt(idxOp, unitaryFunction(idxOp)))(index!, target);
        }
    }

    /// # Summary
    /// Returns a multiply-controlled unitary operation $U$ that applies a
    /// unitary $V_j$ when controlled by n-qubit number state $\ket{j}$.
    ///
    /// $U = \sum^{2^n-1}_{j=0}\ket{j}\bra{j}\otimes V_j$.
    ///
    /// # Input
    /// ## unitaryGenerator
    /// A tuple where the first element `Int` is the number of unitaries $N$,
    /// and the second element `(Int -> ('T => () is Adj + Ctl))`
    /// is a function that takes an integer $j$ in $[0,N-1]$ and outputs the unitary
    /// operation $V_j$.
    ///
    /// # Output
```

```
    /// A multiply-controlled unitary operation $U$ that applies unitaries
    /// described by `unitaryGenerator`.
    ///
    /// # See Also
    /// - Microsoft.Quantum.Canon.MultiplexOperationsFromGenerator
    function MultiplexerFromGenerator(unitaryGenerator : (Int, (Int -> (Qubit[] => Unit is Adj +
Ctl)))) : ((LittleEndian, Qubit[]) => Unit is Adj + Ctl) {
        return MultiplexOperationsFromGenerator(unitaryGenerator, _, _);
    }

    /// # Summary
    /// Returns a multiply-controlled unitary operation $U$ that applies a
    /// unitary $V_j$ when controlled by n-qubit number state $\ket{j}$.
    ///
    /// $U = \sum^{2^n-1}_{j=0}\ket{j}\bra{j}\otimes V_j$.
    ///
    /// # Input
    /// ## unitaryGenerator
    /// A tuple where the first element `Int` is the number of unitaries $N$,
    /// and the second element `(Int -> ('T => () is Adj + Ctl))`
    /// is a function that takes an integer $j$ in $[0,N-1]$ and outputs the unitary
    /// operation $V_j$.
    ///
    /// # Output
    /// A multiply-controlled unitary operation $U$ that applies unitaries
    /// described by `unitaryGenerator`.
    ///
    /// # See Also
    /// - Microsoft.Quantum.Canon.MultiplexOperationsBruteForceFromGenerator
    function MultiplexerBruteForceFromGenerator(unitaryGenerator : (Int, (Int -> (Qubit[] => Unit is
Adj + Ctl)))) : ((LittleEndian, Qubit[]) => Unit is Adj + Ctl) {
        return MultiplexOperationsBruteForceFromGenerator(unitaryGenerator, _, _);
    }

    /// # Summary
    /// Computes a chain of AND gates
    ///
    /// # Description
    /// The auxiliary qubits to compute temporary results must be specified explicitly.
    /// The length of that register is `Length(ctrlRegister) - 2`, if there are at least
    /// two controls, otherwise the length is 0.
    internal operation ApplyAndChain(auxRegister : Qubit[], ctrlRegister : Qubit[], target : Qubit)
    : Unit is Adj {
        if Length(ctrlRegister) == 0 {
            X(target);
        } elif Length(ctrlRegister) == 1 {
            CNOT(Head(ctrlRegister), target);
        } else {
            EqualityFactI(Length(auxRegister), Length(ctrlRegister));
            let controls1 = ctrlRegister[0..0] + auxRegister;
            let controls2 = Rest(ctrlRegister);
            let targets = auxRegister + [target];
            ApplyToEachA(ApplyAnd, Zipped3(controls1, controls2, targets));
        }
    }
}
```

References

1. "Microsoft's Q# quantum programming language out now in preview" (https://arstechnica.com/gadgets/2017/12/microsofts-q-quantum-programming-language-out-now-in-preview/). *Ars Technica*. 12 Dec 2017. Retrieved 2024-09-04.
2. "Introduction to Q#" (https://courses.cs.washington.edu/courses/cse490q/20au/hws/qsharp-intro.pdf) (PDF). University of Washington.

3. QuantumWriter. "The Q# Programming Language" (https://docs.microsoft.com/en-us/quantum/quantum-qr-intro?view=qsharp-preview). *docs.microsoft.com*. Retrieved 2017-12-11.
4. "Announcing the Microsoft Quantum Development Kit" (https://cloudblogs.microsoft.com/quantum/2017/12/11/announcing-microsoft-quantum-development-kit/). Retrieved 2017-12-11.
5. "Microsoft makes play for next wave of computing with quantum computing toolkit" (https://arstechnica.com/gadgets/2017/09/microsoft-quantum-toolkit/). *Ars Technica*. 25 Sep 2017. Retrieved 2024-09-04.
6. "Quantum Computers Barely Exist—Here's Why We're Writing Languages for Them Anyway" (https://www.technologyreview.com/2017/12/22/3662/quantum-computers-barely-exist-heres-why-were-writing-languages-for-them-anyway/). *MIT Technology Review*. 22 Dec 2017. Retrieved 2024-09-04.
7. "Solving the quantum many-body problem with artificial neural networks" (https://cloudblogs.microsoft.com/quantum/2017/02/15/solving-the-quantum-many-body-problem-with-artificial-neural-networks/). *Microsoft Azure Quantum*. 15 February 2017.
8. Scott Aaronson's blog, 2013, 'Microsoft: From QDOS to QMA in less than 35 years', https://scottaaronson.blog/?p=1471
9. "What are the Q# programming language & QDK? - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk). *learn.microsoft.com*. 12 January 2024.
10. "Microsoft announces quantum computing programming language" (https://cloudblogs.microsoft.com/quantum/2017/09/26/microsoft-announces-quantum-computing-programming-language/). Retrieved 2017-12-14.
11. Microsoft is open-sourcing its Quantum Development Kit (https://venturebeat.com/2019/05/06/microsoft-open-sourcing-quantum-development-kit/)
12. Krill, Paul (29 Sep 2020). "Microsoft taps LLVM for quantum computing" (https://www.infoworld.com/article/2260508/microsoft-taps-llvm-for-quantum-computing.html). *InfoWorld*. Retrieved 2024-09-04.
13. "The Women of QuArC" (https://devblogs.microsoft.com/qsharp/the-women-of-quarc/). 30 March 2019.
14. "Intro to Q# - Intro to Quantum Software Development" (https://stem.mitre.org/quantum/software-tools/intro-qsharp.html). *stem.mitre.org*.
15. QuantumWriter. "Setting up the Q# development environment" (https://docs.microsoft.com/en-us/quantum/quantum-installconfig?view=qsharp-preview). *docs.microsoft.com*. Retrieved 2017-12-14.
16. Coppock, Mark (26 Feb 2018). "Microsoft's quantum computing language is now available for MacOS" (https://www.digitaltrends.com/computing/microsoft-quantum-computing-q-available-macos-linux/). *Digital Trends*. Retrieved 2024-09-04.
17. Akdogan, Erman (23 October 2022). "Quantum computing is coming for finance & crypto" (https://medium.datadriveninvestor.com/quantum-computing-is-coming-for-finance-crypto-b56c0255cb09). *Medium*.
18. Melanson, Mike (16 Dec 2017). "This Week in Programming: Get Quantum with Q Sharp" (https://thenewstack.io/week-programming-get-quantum-q-sharp/). *The New Stack*. Retrieved 2024-09-04.
19. "This Week in Programming: Get Quantum with Q Sharp" (https://thenewstack.io/week-programming-get-quantum-q-sharp/). *The New Stack*. 16 December 2017.
20. "Qubit Gate - an overview" (https://www.sciencedirect.com/topics/engineering/qubit-gate). *www.sciencedirect.com*.
21. "Microsoft previews quantum computing development kit" (https://www2.cio.com.au/article/631142/microsoft-previews-quantum-computing-development-kit/). *CIO*.
22. "Types in Q# - Microsoft Quantum" (https://docs.microsoft.com/en-us/quantum/user-guide/language/types). *docs.microsoft.com*. 27 July 2022.

External links

- Official website (https://docs.microsoft.com/en-us/azure/quantum/)
- qsharp-language (https://github.com/microsoft/qsharp-language) on GitHub

Retrieved from "https://en.wikipedia.org/w/index.php?title=Q_Sharp&oldid=1244086803"

WIKIPEDIA
The Free Encyclopedia

libquantum

Libquantum is a C library quantum mechanics simulator originally focused on virtual quantum computers. It is licensed under the GNU GPL. It was a part of SPEC 2006. The latest version is stated to be v1.1.1 (http://www.libquantum.de/files/libquantum-1.1.1.tar.gz) (Jan 2013) on the mailing list, but on the website there is only v0.9.1 from 2007.[1]

An author of libquantum, Hendrik Weimer, has published a paper in *Nature* about using Rydberg atoms for universal quantum simulation with colleagues, using his own work.[2]

References

1. Weimer, Hendrik. "[libquantum-users] Release of libquantum 1.1.1" (http://lists.enyo.de/pipermail/libquantum-users/2013-January/000029.html).
2. Weimer, Hendrik; Müller, Markus; Lesanovsky, Igor; Zoller, Peter; Büchler, Hans Peter (14 March 2010). "A Rydberg quantum simulator". *Nature Physics*. **6** (5): 382–388. arXiv:0907.1657 (https://arxiv.org/abs/0907.1657). Bibcode:2010NatPh...6..382W (https://ui.adsabs.harvard.edu/abs/2010NatPh...6..382W). doi:10.1038/nphys1614 (https://doi.org/10.1038%2Fnphys1614). S2CID 54710282 (https://api.semanticscholar.org/CorpusID:54710282).

External links

- libquantum homepage (http://www.libquantum.de/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Libquantum&oldid=1238715361"

WIKIPEDIA
The Free Encyclopedia

Quantum programming

Quantum programming is the process of designing or assembling sequences of instructions, called quantum circuits, using gates, switches, and operators to manipulate a quantum system for a desired outcome or results of a given experiment. Quantum circuit algorithms can be implemented on integrated circuits, conducted with instrumentation, or written in a programming language for use with a quantum computer or a quantum processor.

With quantum processor based systems, quantum programming languages help express quantum algorithms using high-level constructs.[1] The field is deeply rooted in the open-source philosophy and as a result most of the quantum software discussed in this article is freely available as open-source software.[2]

Quantum computers, such as those based on the KLM protocol, a linear optical quantum computing (LOQC) model, use quantum algorithms (circuits) implemented with electronics, integrated circuits, instrumentation, sensors, and/or by other physical means.

Other circuits designed for experimentation related to quantum systems can be instrumentation and sensor based.

Quantum instruction sets

Quantum instruction sets are used to turn higher level algorithms into physical instructions that can be executed on quantum processors. Sometimes these instructions are specific to a given hardware platform, e.g. ion traps or superconducting qubits.

Blackbird

Blackbird[3][4] is a quantum instruction set and intermediate representation used by Xanadu Quantum Technologies and Strawberry Fields. It is designed to represent continuous-variable quantum programs that can run on photonic quantum hardware.

cQASM

cQASM,[5] also known as common QASM, is a hardware-agnostic quantum assembly language which guarantees the interoperability between all the quantum compilation and simulation tools. It was introduced by the QCA Lab at TUDelft.

OpenQASM

OpenQASM[6] is the intermediate representation introduced by IBM for use with Qiskit and the IBM Q Experience.

Quil

Quil is an instruction set architecture for quantum computing that first introduced a shared quantum/classical memory model. It was introduced by Robert Smith, Michael Curtis, and William Zeng in *A Practical Quantum Instruction Set Architecture*.[7] Many quantum algorithms (including quantum teleportation, quantum error correction, simulation,[8][9] and optimization algorithms[10]) require a shared memory architecture.

Quantum software development kits

Quantum software development kits provide collections of tools to create and manipulate quantum programs.[11] They also provide the means to simulate the quantum programs or prepare them to be run using cloud-based quantum devices and self-hosted quantum devices.

SDKs with access to quantum processors

The following software development kits can be used to run quantum circuits on prototype quantum devices, as well as on simulators.

Cirq

An open source project developed by Google, which uses the Python programming language to create and manipulate quantum circuits. Programs written in Cirq can be run on IonQ, Pasqal,[12] Rigetti, and Alpine Quantum Technologies.[13]

Classiq

A cloud-based quantum IDE developed by Classiq, uses a high-level quantum language, Qmod, to generate scalable and efficient quantum circuits with a hardware-aware synthesis engine, that can be deployed across a wide range of QPUs. The platform includes a large library of quantum algorithms.

Forest

An open source project developed by Rigetti, which uses the Python programming language to create and manipulate quantum circuits. Results are obtained either using simulators or prototype quantum devices provided by Rigetti. As well as the ability to create programs using basic quantum operations, higher level algorithms are available within the Grove package.[14] Forest is based on the Quil instruction set.

MindQuantum

MindQuantum is a quantum computing framework based on MindSpore, focusing on the implementation of NISQ algorithms.[15][16][17]

Ocean

An open source suite of tools developed by D-Wave. Written mostly in the Python programming language, it enables users to formulate problems in Ising Model and Quadratic Unconstrained Binary Optimization formats (QUBO). Results can be obtained by submitting to an online quantum computer in Leap, D-Wave's real-time Quantum Application Environment, customer-owned machines, or classical samplers.

PennyLane

An open-source Python library developed by Xanadu Quantum Technologies for differentiable programming of quantum computers.[18][19][20][21] PennyLane provides users the ability to create models using TensorFlow, NumPy, or PyTorch, and connect them with quantum computer backends available from IBMQ, Google Quantum, Rigetti, Quantinuum[22] and Alpine Quantum Technologies.[13][23]

```python
from projectq import MainEngine        # import the main compiler engine
from projectq.ops import H, Measure, X # import the operations we want to
                                       # perform (Hadamard, X, measurement)

eng = MainEngine()   # create a default compiler (the backend is a simulator)
qubit = eng.allocate_qubit() # allocate 1 qubit

H | qubit # apply a Hadamard gate
X | qubit # apply an X gate
Measure | qubit # measure the qubit

eng.flush() # flush all gates (and execute measurements)
print("Measured {}".format(int(qubit))) # output measurement result

#
# Output: "Measured 1"
#
# Note that this is the (slow) Python simulator.
```

A sample code using projectq with Python

Perceval

An open-source project created by Quandela for designing photonic quantum circuits and developing quantum algorithms, based on Python. Simulations are run either on the user's own computer or on the cloud. Perceval is also used to connect to Quandela's cloud-based photonic quantum processor.[24][25]

ProjectQ

An open source project developed at the Institute for Theoretical Physics at ETH, which uses the Python programming language to create and manipulate quantum circuits.[26] Results are obtained either using a simulator, or by sending jobs to IBM quantum devices.

Qibo

An open source full-stack API for quantum simulation, quantum hardware control and calibration developed by multiple research laboratories, including QRC, CQT and INFN. Qibo (https://github.com/qiboteam/qibo) is a modular framework which includes multiple backends for quantum simulation and hardware control.[27][28] This project aims at providing a platform agnostic quantum hardware control framework with drivers for multiple instruments[29] and tools for quantum calibration, characterization and validation.[30] This framework focuses on self-hosted quantum devices by simplifying the software development required in labs.

Qiskit

An open source project developed by IBM.[31] Quantum circuits are created and manipulated using Python. Results are obtained either using simulators that run on the user's own device, simulators provided by IBM or prototype quantum devices provided by IBM. As well as the ability to create

programs using basic quantum operations, higher level tools for algorithms and benchmarking are available within specialized packages.[32] Qiskit is based on the OpenQASM standard for representing quantum circuits. It also supports pulse level control of quantum systems via QiskitPulse standard.[33]

Qrisp

Qrisp[34] is an open source project coordinated by the Eclipse Foundation[35] and developed in Python programming by Fraunhofer FOKUS[36] Qrisp is a high-level programming language for creating and compiling quantum algorithms. Its structured programming model enables scalable development and maintenance. The expressive syntax is based on variables instead of qubits, with the QuantumVariable as core class, and functions instead of gates. Additional tools, such as a performant simulator and automatic uncomputation, complement the extensive framework. Furthermore, it is platform independent, since it offers alternative compilation of elementary functions down to the circuit level, based on device-specific gate sets.

Quantum Development Kit

A project developed by Microsoft[37] as part of the .NET Framework. Quantum programs can be written and run within Visual Studio and VSCode using the quantum programming language Q#. Programs developed in the QDK can be run on Microsoft's Azure Quantum,[38] and run on quantum computers from Quantinuum,[22] IonQ, and Pasqal.[12]

Strawberry Fields

An open-source Python library developed by Xanadu Quantum Technologies for designing, simulating, and optimizing continuous variable (CV) quantum optical circuits.[39][40] Three simulators are provided - one in the Fock basis, one using the Gaussian formulation of quantum optics,[41] and one using the TensorFlow machine learning library. Strawberry Fields is also the library for executing programs on Xanadu's quantum photonic hardware.[42][43]

t|ket>

A quantum programming environment and optimizing compiler developed by Cambridge Quantum Computing that targets simulators and several quantum hardware back-ends, released in December 2018.[44]

Quantum programming languages

There are two main groups of quantum programming languages: imperative quantum programming languages and functional quantum programming languages.

Imperative languages

The most prominent representatives of the imperative languages are QCL,[45] LanQ[46] and Q|SI>.[47]

Ket

Ket[48] is an open-source embedded language designed to facilitate quantum programming, leveraging the familiar syntax and simplicity of Python. It serves as an integral component of the Ket Quantum Programming Platform,[49] seamlessly integrating with a Rust runtime library and a quantum simulator. Maintained by Quantuloop, the project emphasizes accessibility and versatility for researchers and developers. The following example demonstrates the implementation of a Bell state using Ket:

```
from ket import *
a, b = quant(2) # Allocate two quantum bits
H(a) # Put qubit `a` in a superposition
cnot(a, b) # Entangle the two qubits in the Bell state
m_a = measure(a) # Measure qubit `a`, collapsing qubit `b` as well
m_b = measure(b) # Measure qubit `b`
# Assert that the measurement of both qubits will always be equal
assert m_a.value == m_b.value
```

LQP

The Logic of Quantum Programs (LQP) is a dynamic quantum logic, capable of expressing important features of quantum measurements and unitary evolutions of multi-partite states, and provides logical characterizations of various forms of entanglement. The logic has been used to specify and verify the correctness of various protocols in quantum computation.[50][51]

Q language

Q Language is the second implemented imperative quantum programming language.[52] Q Language was implemented as an extension of C++ programming language. It provides classes for basic quantum operations like QHadamard, QFourier, QNot, and QSwap, which are derived from the base class Qop. New operators can be defined using C++ class mechanism.

Quantum memory is represented by class Qreg.

```
Qreg x1; // 1-qubit quantum register with initial value 0
Qreg x2(2,0); // 2-qubit quantum register with initial value 0
```

The computation process is executed using a provided simulator. Noisy environments can be simulated using parameters of the simulator.

Q#

A language developed by Microsoft to be used with the Quantum Development Kit.[53]

QCL

Quantum Computation Language (QCL) is one of the first implemented quantum programming languages.[54] The most important feature of QCL is the support for user-defined operators and functions. Its syntax resembles the syntax of the C programming language and its classical data types are similar to primitive data types in C. One can combine classical code and quantum code in the same program.

qGCL

Quantum Guarded Command Language (qGCL) was defined by P. Zuliani in his PhD thesis. It is based on Guarded Command Language created by Edsger Dijkstra.

It can be described as a language of quantum programs specification.

QMASM

Quantum Macro Assembler (QMASM) is a low-level language specific to quantum annealers such as the D-Wave.[55]

Qmod

Quantum Modeling (Qmod) language is a high-level language that abstracts away the gate-level qubit operation, providing a functional approach to the implementation of quantum algorithms on quantum registers. The language is part of the Classiq (https://classiq.io) platform and can be used directly with its native syntax, through a Python SDK, or with a visual editor, all methods can take advantage of the larger library of algorithms and the efficient circuit optimization.

Q|SI>

Q|SI> is a platform embedded in .Net language supporting quantum programming in a quantum extension of while-language.[47][56] This platform includes a compiler of the quantum while-language[57] and a chain of tools for the simulation of quantum computation, optimisation of quantum circuits, termination analysis of quantum programs,[58] and verification of quantum programs.[59][60]

Quantum pseudocode

Quantum pseudocode proposed by E. Knill is the first formalized language for description of quantum algorithms. It was introduced and, moreover, was tightly connected with a model of quantum machine called Quantum Random Access Machine (QRAM).

Scaffold

Scaffold is C-like language, that compiles to QASM and OpenQASM. It is built on top of the LLVM Compiler Infrastructure to perform optimizations on Scaffold code before generating a specified instruction set.[61][62]

Silq

Silq is a high-level programming language for quantum computing with a strong static type system, developed at ETH Zürich.[63][64]

Functional languages

Efforts are underway to develop functional programming languages for quantum computing. Functional programming languages are well-suited for reasoning about programs. Examples include Selinger's QPL,[65] and the Haskell-like language QML by Altenkirch and Grattage.[66][67] Higher-order quantum programming languages, based on lambda calculus, have been proposed by van Tonder,[68] Selinger and Valiron[69] and by Arrighi and Dowek.[70]

LIQUi|>

LIQUi|> (pronounced *liquid*) is a quantum simulation extension on the F# programming language.[71] It is currently being developed by the Quantum Architectures and Computation Group (QuArC)[72] part of the StationQ efforts at Microsoft Research. LIQUi|> seeks to allow theorists to experiment with quantum algorithm design before physical quantum computers are available for use.[73]

It includes a programming language, optimization and scheduling algorithms, and quantum simulators. LIQUi|> can be used to translate a quantum algorithm written in the form of a high-level program into the low-level machine instructions for a quantum device.[74]

QFC and QPL

QFC and QPL are two closely related quantum programming languages defined by Peter Selinger. They differ only in their syntax: QFC uses a flow chart syntax, whereas QPL uses a textual syntax. These languages have classical control flow but can operate on quantum or classical data. Selinger gives a denotational semantics for these languages in a category of superoperators.

QML

QML is a Haskell-like quantum programming language by Altenkirch and Grattage.[75][66] Unlike Selinger's QPL, this language takes duplication, rather than discarding, of quantum information as a primitive operation. Duplication in this context is understood to be the operation that maps $|\phi\rangle$ to $|\phi\rangle \otimes |\phi\rangle$, and is not to be confused with the impossible operation of cloning; the authors claim it is akin to how sharing is modeled in classical languages. QML also introduces both classical and quantum control operators, whereas most other languages rely on classical control.

An operational semantics for QML is given in terms of quantum circuits, while a denotational semantics is presented in terms of superoperators, and these are shown to agree. Both the operational and denotational semantics have been implemented (classically) in Haskell.[76]

Quantum lambda calculi

Quantum lambda calculi are extensions of the classical lambda calculus introduced by Alonzo Church and Stephen Cole Kleene in the 1930s. The purpose of quantum lambda calculi is to extend quantum programming languages with a theory of higher-order functions.

The first attempt to define a quantum lambda calculus was made by Philip Maymin in 1996.[77] His lambda-q calculus is powerful enough to express any quantum computation. However, this language can efficiently solve NP-complete problems, and therefore appears to be strictly stronger than the standard

quantum computational models (such as the quantum Turing machine or the quantum circuit model). Therefore, Maymin's lambda-q calculus is probably not implementable on a physical device .

In 2003, André van Tonder defined an extension of the lambda calculus suitable for proving correctness of quantum programs. He also provided an implementation in the Scheme programming language.[78]

In 2004, Selinger and Valiron defined a strongly typed lambda calculus for quantum computation with a type system based on linear logic.[79]

Quipper

Quipper was published in 2013.[80][81] It is implemented as an embedded language, using Haskell as the host language.[82] For this reason, quantum programs written in Quipper are written in Haskell using provided libraries. For example, the following code implements preparation of a superposition

```
import Quipper

spos :: Bool -> Circ Qubit
spos b = do q <- qinit b
            r <- hadamard q
            return r
```

References

1. Jarosław Adam Miszczak (2012). *High-level Structures in Quantum Computing*. Morgan & Claypool Publishers. ISBN 9781608458516.
2. "Comprehensive list of quantum open-source projects" (https://github.com/qosf/awesome-quantum-software). *Github*. Retrieved January 27, 2022.
3. "Blackbird Quantum Assembly Language — Blackbird 0.2.0 documentation" (https://quantum-blackbird.readthedocs.io/en/latest/). *quantum-blackbird.readthedocs.io*. Retrieved June 24, 2019.
4. Weedbrook, Christian; Amy, Matthew; Bergholm, Ville; Quesada, Nicolás; Izaac, Josh; Killoran, Nathan (March 11, 2019). "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum*. **3**: 129. arXiv:1804.03159 (https://arxiv.org/abs/1804.03159). Bibcode:2019Quant...3..129K (https://ui.adsabs.harvard.edu/abs/2019Quant...3..129K). doi:10.22331/q-2019-03-11-129 (https://doi.org/10.22331%2Fq-2019-03-11-129). S2CID 54763305 (https://api.semanticscholar.org/CorpusID:54763305).
5. Bertels, K.; Almudever, C. G.; Hogaboam, J. W.; Ashraf, I.; Guerreschi, G. G.; Khammassi, N. (May 24, 2018). "cQASM v1.0: Towards a Common Quantum Assembly Language". arXiv:1805.09607v1 (https://arxiv.org/abs/1805.09607v1) [quant-ph (https://arxiv.org/archive/quant-ph)].
6. *qiskit-openqasm: OpenQASM specification* (https://github.com/IBM/qiskit-openqasm), International Business Machines, July 4, 2017, retrieved July 6, 2017
7. Smith, Robert S.; Curtis, Michael J.; Zeng, William J. (2016). "A Practical Quantum Instruction Set Architecture". arXiv:1608.03355 (https://arxiv.org/abs/1608.03355) [quant-ph (https://arxiv.org/archive/quant-ph)].

8. McClean, Jarrod R.; Romero, Jonathan; Babbush, Ryan; Aspuru-Guzik, Alán (February 4, 2016). "The theory of variational hybrid quantum-classical algorithms". *New Journal of Physics*. **18** (2): 023023. arXiv:1509.04279 (https://arxiv.org/abs/1509.04279). Bibcode:2016NJPh...18b3023M (https://ui.adsabs.harvard.edu/abs/2016NJPh...18b3023M). doi:10.1088/1367-2630/18/2/023023 (https://doi.org/10.1088%2F1367-2630%2F18%2F2%2F023023). ISSN 1367-2630 (https://search.worldcat.org/issn/1367-2630). S2CID 92988541 (https://api.semanticscholar.org/CorpusID:92988541).
9. Rubin, Nicholas C.; Curtis, Michael J.; Zeng, William J. (2016). "A Hybrid Classical/Quantum Approach for Large-Scale Studies of Quantum Systems with Density Matrix Embedding Theory". arXiv:1610.06910 (https://arxiv.org/abs/1610.06910) [quant-ph (https://arxiv.org/archive/quant-ph)].
10. Farhi, Edward; Goldstone, Jeffrey; Gutmann, Sam (2014). "A Quantum Approximate Optimization Algorithm". arXiv:1411.4028 (https://arxiv.org/abs/1411.4028) [quant-ph (https://arxiv.org/archive/quant-ph)].
11. Häner, Thomas; Steiger, Damian S.; Svore, Krysta; Troyer, Matthias (2018). "A software methodology for compiling quantum programs". *Quantum Science and Technology*. **3** (2): 020501. arXiv:1604.01401 (https://arxiv.org/abs/1604.01401). Bibcode:2018QS&T....3b0501H (https://ui.adsabs.harvard.edu/abs/2018QS&T....3b0501H). doi:10.1088/2058-9565/aaa5cc (https://doi.org/10.1088%2F2058-9565%2Faaa5cc). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 1922315 (https://api.semanticscholar.org/CorpusID:1922315).
12. "PASQAL" (https://pasqal.io/). *PASQAL*.
13. "Home" (https://www.aqt.eu/). *AQT | ALPINE QUANTUM TECHNOLOGIES*.
14. "Welcome to the Documentation for Grove! — Grove 1.7.0 documentation" (https://grove-docs.readthedocs.io/en/latest/). *grove-docs.readthedocs.io*.
15. "MindSpore Quantum Documentation" (https://www.mindspore.cn/mindquantum/docs/en/master/index.html). *www.mindspore.cn/mindquantum*.
16. Xu, Xusheng; et al. (2024). "MindSpore Quantum: A User-Friendly, High-Performance, and AI-Compatible Quantum Computing Framework". arXiv:2406.17248 (https://arxiv.org/abs/2406.17248) [quant-ph (https://arxiv.org/archive/quant-ph)].
17. "mindquantum" (https://github.com/mindspore-ai/mindquantum). *github.com*.
18. "PennyLane Documentation — PennyLane 0.14.1 documentation" (https://pennylane.readthedocs.io/en/stable/). *pennylane.readthedocs.io*. Retrieved March 26, 2021.
19. "AWS joins PennyLane, an open-source framework that melds machine learning with quantum computing" (https://siliconangle.com/2021/02/17/aws-throws-weight-behind-pennylane-open-source-framework-melds-machine-learning-quantum-computing/). *SiliconANGLE*. February 17, 2021. Retrieved March 26, 2021.
20. "SD Times Open-Source Project of the Week: PennyLane" (https://sdtimes.com/open-source/sd-times-open-source-project-of-the-week-pennylane/). *SD Times*. February 26, 2021. Retrieved March 26, 2021.
21. Salamone, Salvatore (December 13, 2020). "Real-time Analytics News Roundup for Week Ending December 12" (https://www.rtinsights.com/real-time-analytics-news-roundup-for-week-ending-december-12/). *RTInsights*. Retrieved March 26, 2021.
22. "Accelerating Quantum Computing" (https://www.quantinuum.com/). *www.quantinuum.com*.
23. "Plugins and ecosystem — PennyLane" (https://pennylane.ai/plugins.html). *pennylane.ai*. Retrieved March 26, 2021.
24. "La puissance d'un ordinateur quantique testée en ligne (The power of a quantum computer tested online)" (https://www.lemonde.fr/sciences/article/2022/11/22/la-puissance-d-un-ordinateur-quantique-testee-en-ligne_6151063_1650684.html). *Le Monde.fr*. Le Monde. November 22, 2022.

25. Heurtel, Nicolas; Fyrillas, Andreas; de Gliniasty, Grégoire; Le Bihan, Raphaël; Malherbe, Sébastien; Pailhas, Marceau; Bertasi, Eric; Bourdoncle, Boris; Emeriau, Pierre-Emmanuel; Mezher, Rawad; Music, Luka; Belabas, Nadia; Valiron, Benoît; Senellart, Pascale; Mansfield, Shane; Senellart, Jean (February 21, 2023). "Perceval: A Software Platform for Discrete Variable Photonic Quantum Computing" (https://quantum-journal.org/papers/q-2023-02-21-931/). *Quantum*. **7**: 931. arXiv:2204.00602 (https://arxiv.org/abs/2204.00602). Bibcode:2023Quant...7..931H (https://ui.adsabs.harvard.edu/abs/2023Quant...7..931H). doi:10.22331/q-2023-02-21-931 (https://doi.org/10.22331%2Fq-2023-02-21-931). S2CID 247922568 (https://api.semanticscholar.org/CorpusID:247922568).
26. "Home" (https://projectq.ch/).
27. Efthymiou, Stavros; Ramos-Calderer, Sergi; Bravo-Prieto, Carlos; Pérez-Salinas, Adrián; García-Martín, Diego; Garcia-Saez, Artur; Latorre, José Ignacio; Carrazza, Stefano (January 1, 2022). "Qibo: a framework for quantum simulation with hardware acceleration" (https://iopscience.iop.org/article/10.1088/2058-9565/ac39f5). *Quantum Science and Technology*. **7** (1): 015018. arXiv:2009.01845 (https://arxiv.org/abs/2009.01845). Bibcode:2022QS&T....7a5018E (https://ui.adsabs.harvard.edu/abs/2022QS&T....7a5018E). doi:10.1088/2058-9565/ac39f5 (https://doi.org/10.1088%2F2058-9565%2Fac39f5). hdl:2434/887963 (https://hdl.handle.net/2434%2F887963). ISSN 2058-9565 (https://search.worldcat.org/issn/2058-9565). S2CID 221507478 (https://api.semanticscholar.org/CorpusID:221507478).
28. Efthymiou, Stavros; Lazzarin, Marco; Pasquale, Andrea; Carrazza, Stefano (September 22, 2022). "Quantum simulation with just-in-time compilation" (https://quantum-journal.org/papers/q-2022-09-22-814/). *Quantum*. **6**: 814. arXiv:2203.08826 (https://arxiv.org/abs/2203.08826). Bibcode:2022Quant...6..814E (https://ui.adsabs.harvard.edu/abs/2022Quant...6..814E). doi:10.22331/q-2022-09-22-814 (https://doi.org/10.22331%2Fq-2022-09-22-814). S2CID 247518955 (https://api.semanticscholar.org/CorpusID:247518955).
29. "Qibolab" (https://github.com/qiboteam/qibolab). November 2, 2022 – via GitHub.
30. "Qibocal" (https://github.com/qiboteam/qibocal). November 1, 2022 – via GitHub.
31. "qiskit.org" (https://qiskit.org/). *qiskit.org*.
32. "Qiskit Overview" (https://qiskit.org/overview/). Retrieved February 10, 2021.
33. McKay, David C.; Alexander, Thomas; Bello, Luciano; Biercuk, Michael J.; Bishop, Lev; Chen, Jiayin; Chow, Jerry M.; Córcoles, Antonio D.; Egger, Daniel; Filipp, Stefan; Gomez, Juan; Hush, Michael; Javadi-Abhari, Ali; Moreda, Diego; Nation, Paul; Paulovicks, Brent; Winston, Erick; Wood, Christopher J.; Wootton, James; Gambetta, Jay M. (2018). "Qiskit Backend Specifications for OpenQASM and OpenPulse Experiments". arXiv:1809.03452 (https://arxiv.org/abs/1809.03452) [quant-ph (https://arxiv.org/archive/quant-ph)].
34. "Qrisp official website" (https://www.qrisp.eu/).
35. "Eclipse Foundation (website)" (https://www.eclipse.org/org/foundation/).
36. "Fraunhofer FOKUS (website)" (https://www.fokus.fraunhofer.de/).
37. "Azure Quantum documentation, QDK & Q# API reference - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/). *learn.microsoft.com*.
38. "What is Azure Quantum? - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum). *learn.microsoft.com*. January 11, 2023.
39. "Strawberry Fields — Strawberry Fields 0.8.0 documentation" (https://strawberryfields.readthedocs.io/en/latest/). *strawberryfields.readthedocs.io*. Retrieved September 25, 2018.
40. Killoran, Nathan; Izaac, Josh; Quesada, Nicolás; Bergholm, Ville; Amy, Matthew; Weedbrook, Christian (2019). "Strawberry Fields: A Software Platform for Photonic Quantum Computing". *Quantum*. **3**: 129. arXiv:1804.03159 (https://arxiv.org/abs/1804.03159). Bibcode:2019Quant...3..129K (https://ui.adsabs.harvard.edu/abs/2019Quant...3..129K). doi:10.22331/q-2019-03-11-129 (https://doi.org/10.22331%2Fq-2019-03-11-129). S2CID 54763305 (https://api.semanticscholar.org/CorpusID:54763305).

41. Weedbrook, Christian; Pirandola, Stefano; García-Patrón, Raúl; Cerf, Nicolas J.; Ralph, Timothy C.; Shapiro, Jeffrey H.; Lloyd, Seth (May 1, 2012). "Gaussian quantum information". *Reviews of Modern Physics*. **84** (2): 621–669. arXiv:1110.3234 (https://arxiv.org/abs/1110.3234). Bibcode:2012RvMP...84..621W (https://ui.adsabs.harvard.edu/abs/2012RvMP...84..621W). doi:10.1103/RevModPhys.84.621 (https://doi.org/10.1103%2FRevModPhys.84.621). S2CID 119250535 (https://api.semanticscholar.org/CorpusID:119250535).
42. "Hardware — Strawberry Fields" (https://strawberryfields.ai/photonics/hardware/index.html). *strawberryfields.ai*. Retrieved March 26, 2021.
43. "In the Race to Hundreds of Qubits, Photons May Have "Quantum Advantage" " (https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon). *IEEE Spectrum: Technology, Engineering, and Science News*. March 5, 2021. Retrieved March 26, 2021.
44. "pytket" (https://github.com/CQCL/pytket). *GitHub*. January 22, 2022.
45. Bernhard Omer. "The QCL Programming Language" (http://tph.tuwien.ac.at/~oemer/qcl.html).
46. Hynek Mlnařík. "LanQ – a quantum imperative programming language" (http://lanq.sourceforge.net/).
47. Liu, Shusen; Zhou, li; Guan, Ji; He, Yang; Duan, Runyao; Ying, Mingsheng (May 9, 2017). "Q|SI>: A Quantum Programming Language". *Scientia Sinica Informationis*. **47** (10): 1300. arXiv:1710.09500 (https://arxiv.org/abs/1710.09500). doi:10.1360/N112017-00095 (https://doi.org/10.1360%2FN112017-00095). S2CID 9163705 (https://api.semanticscholar.org/CorpusID:9163705).
48. Da Rosa, Evandro Chagas Ribeiro; De Santiago, Rafael (January 31, 2022). "Ket Quantum Programming" (https://dl.acm.org/doi/10.1145/3474224). *ACM Journal on Emerging Technologies in Computing Systems*. **18** (1): 1–25. doi:10.1145/3474224 (https://doi.org/10.1145%2F3474224). ISSN 1550-4832 (https://search.worldcat.org/issn/1550-4832).
49. "Ket Quantum Programming" (https://quantumket.org). *quantumket.org*. Retrieved May 18, 2023.
50. A. Baltag and S. Smets, "LQP: The Dynamic Logic of Quantum Information" (https://arxiv.org/abs/2110.01361), Mathematical Structures in Computer Science 16(3):491-525, 2006.
51. Baltag, Alexandru; Bergfeld, Jort; Kishida, Kohei; Sack, Joshua; Smets, Sonja; Zhong, Shengyang (2014). "PLQP & Company: Decidable Logics for Quantum Algorithms" (https://link.springer.com/article/10.1007/s10773-013-1987-3). *International Journal of Theoretical Physics*. **53** (10): 3628–3647. Bibcode:2014IJTP...53.3628B (https://ui.adsabs.harvard.edu/abs/2014IJTP...53.3628B). doi:10.1007/s10773-013-1987-3 (https://doi.org/10.1007%2Fs10773-013-1987-3). S2CID 254573992 (https://api.semanticscholar.org/CorpusID:254573992).
52. "Software for the Q language" (https://web.archive.org/web/20090620011647/http://sra.itc.it/people/serafini/qlang/). November 23, 2001. Archived from the original (http://sra.itc.it/people/serafini/qlang/) on June 20, 2009. Retrieved July 20, 2017.
53. "Introduction to Q# & Quantum Development Kit - Azure Quantum" (https://learn.microsoft.com/en-us/azure/quantum/overview-what-is-qsharp-and-qdk). *learn.microsoft.com*. March 30, 2023.
54. "QCL - A Programming Language for Quantum Computers" (http://tph.tuwien.ac.at/~oemer/qcl.html). *tuwien.ac.at*. Retrieved July 20, 2017.
55. Scott Pakin, "A Quantum Macro Assembler" (https://ieeexplore.ieee.org/document/7761637/), Proceedings of the 20th Annual IEEE High Performance Extreme Computing Conference 2016
56. Ying, Mingsheng (January 2012). "Floyd–hoare Logic for Quantum Programs" (https://doi.org/10.1145%2F2049706.2049708). *ACM Trans. Program. Lang. Syst*. **33** (6): 19:1–19:49. doi:10.1145/2049706.2049708 (https://doi.org/10.1145%2F2049706.2049708). ISSN 0164-0925 (https://search.worldcat.org/issn/0164-0925). S2CID 416960 (https://api.semanticscholar.org/CorpusID:416960).

57. Ying, Mingsheng; Feng, Yuan (2010). "A Flowchart Language for Quantum Programming" (https://www.computer.org/csdl/trans/ts/2011/04/tts2011040466-abs.html). *IEEE Transactions on Software Engineering*. **37** (4): 466–485. doi:10.1109/TSE.2010.94 (https://doi.org/10.1109%2FTSE.2010.94). ISSN 0098-5589 (https://search.worldcat.org/issn/0098-5589). S2CID 5879273 (https://api.semanticscholar.org/CorpusID:5879273).
58. Ying, Mingsheng; Yu, Nengkun; Feng, Yuan; Duan, Runyao (2013). "Verification of quantum programs". *Science of Computer Programming*. **78** (9): 1679–1700. arXiv:1106.4063 (https://arxiv.org/abs/1106.4063). doi:10.1016/j.scico.2013.03.016 (https://doi.org/10.1016%2Fj.scico.2013.03.016). S2CID 18913620 (https://api.semanticscholar.org/CorpusID:18913620).
59. Ying, Mingsheng; Ying, Shenggang; Wu, Xiaodi (2017), "Invariants of quantum programs: Characterisations and generation", *ACM SIGPLAN Notices*, **52**: 818–832, doi:10.1145/3093333.3009840 (https://doi.org/10.1145%2F3093333.3009840), hdl:10453/127333 (https://hdl.handle.net/10453%2F127333)
60. Liu, Tao; Li, Yangjia; Wang, Shuling; Ying, Mingsheng; Zhan, Naijun (2016). "A Theorem Prover for Quantum Hoare Logic and its Applications". arXiv:1601.03835 (https://arxiv.org/abs/1601.03835) [cs.LO (https://arxiv.org/archive/cs.LO)].
61. Javadi-Abhari, Ali. "Scaffold: Quantum Programming Language" (https://www.cs.princeton.edu/research/techreps/TR-934-12). *Princeton University-Department of Computer Science*. Princeton University. Retrieved September 22, 2020.
62. Litteken, Andrew (May 28, 2020). "An updated LLVM-based quantum research compiler with further OpenQASM support" (https://doi.org/10.1088%2F2058-9565%2Fab8c2c). *Quantum Science and Technology*. **5** (3): 034013. Bibcode:2020QS&T....5c4013L (https://ui.adsabs.harvard.edu/abs/2020QS&T....5c4013L). doi:10.1088/2058-9565/ab8c2c (https://doi.org/10.1088%2F2058-9565%2Fab8c2c). OSTI 1803951 (https://www.osti.gov/biblio/1803951). S2CID 219101628 (https://api.semanticscholar.org/CorpusID:219101628).
63. "What is Silq?" (https://silq.ethz.ch/). *silq.ethz.ch*. Retrieved June 21, 2020.
64. Bichsel, Benjamin; Baader, Maximilian; Gehr, Timon; Vechev, Martin (June 11, 2020). "Silq: A high-level quantum language with safe uncomputation and intuitive semantics". *Proceedings of the 41st ACM SIGPLAN Conference on Programming Language Design and Implementation*. London UK: ACM. pp. 286–300. doi:10.1145/3385412.3386007 (https://doi.org/10.1145%2F3385412.3386007). ISBN 978-1-4503-7613-6. S2CID 219397029 (https://api.semanticscholar.org/CorpusID:219397029).
65. Peter Selinger, "Towards a quantum programming language" (http://www.mathstat.dal.ca/~selinger/papers.html#qpl), Mathematical Structures in Computer Science 14(4):527-586, 2004.
66. Jonathan Grattage: QML Research (http://www.cs.nott.ac.uk/~jjg/qml.html) (website)
67. T. Altenkirch, V. Belavkin, J. Grattage, A. Green, A. Sabry, J. K. Vizzotto, QML: A Functional Quantum Programming Language (http://sneezy.cs.nott.ac.uk/qml) Archived (https://web.archive.org/web/20060710201728/http://sneezy.cs.nott.ac.uk/QML/) 2006-07-10 at the Wayback Machine (website)
68. Andre van Tonder, "A Lambda Calculus for Quantum Computation" (https://dx.doi.org/10.1137/S0097539703432165), SIAM J. Comput., 33(5), 1109–1135. (27 pages), 2004. Also available from arXiv:quant-ph/0307150 (https://arxiv.org/abs/quant-ph/0307150)
69. Peter Selinger and Benoît Valiron, "A lambda calculus for quantum computation with classical control" (http://www.mathstat.dal.ca/~selinger/papers/#qlambda), Mathematical Structures in Computer Science 16(3):527-552, 2006.
70. Pablo Arrighi, Gilles Dowek, "Linear-algebraic lambda-calculus: higher-order, encodings and confluence" (http://www.arxiv.org/abs/quant-ph/0612199), 2006
71. "The Language Integrated Quantum Operations Simulator" (https://stationq.github.io/Liquid/). *github.io*. Retrieved July 20, 2017.
72. Quantum Architectures and Computation Group (QuArC), https://www.microsoft.com/en-us/research/group/quantum-architectures-and-computation-group-quarc/, 2011

73. "StationQ" (https://stationq.microsoft.com/). *microsoft.com*. Retrieved July 20, 2017.
74. "Language-Integrated Quantum Operations: LIQUi|>" (https://www.microsoft.com/en-us/research/project/language-integrated-quantum-operations-liqui/). *Microsoft*. 2016.
75. "QML: A Functional Quantum Programming Language" (https://web.archive.org/web/20070926230222/http://sneezy.cs.nott.ac.uk/QML/). September 26, 2007. Archived from the original (http://sneezy.cs.nott.ac.uk/QML/) on September 26, 2007.
76. Jonathan Grattage, QML: A Functional Quantum Programming Language (compiler) (http://sneezy.cs.nott.ac.uk/qml/compiler) Archived (https://web.archive.org/web/20160305052237/http://sneezy.cs.nott.ac.uk/qml/compiler/) 2016-03-05 at the Wayback Machine, 2005–2008
77. Philip Maymin, "Extending the Lambda Calculus to Express Randomized and Quantumized Algorithms" (https://arxiv.org/abs/quant-ph/9612052), 1996
78. André van Tonder. "A lambda calculus for quantum computation (website)" (https://web.archive.org/web/20160305100936/http://www.het.brown.edu/people/andre/qlambda/). Archived from the original (http://www.het.brown.edu/people/andre/qlambda) on March 5, 2016. Retrieved October 2, 2007.
79. Peter Selinger, Benoˆıt Valiron, "Quantum Lambda Calculus" (https://www.mscs.dal.ca/~selinger/papers/qlambdabook.pdf)
80. "The Quipper Language" (http://www.mathstat.dal.ca/~selinger/quipper/).
81. Alexander S. Green; Peter LeFanu Lumsdaine; Neil J. Ross; Peter Selinger; Benoît Valiron. "The Quipper Language (website)" (http://www.mathstat.dal.ca/~selinger/quipper/).
82. Alexander S. Green; Peter LeFanu Lumsdaine; Neil J. Ross; Peter Selinger; Benoît Valiron (2013). "An Introduction to Quantum Programming in Quipper". *Reversible Computation*. Lecture Notes in Computer Science. Vol. 7948. pp. 110–124. arXiv:1304.5485 (https://arxiv.org/abs/1304.5485). doi:10.1007/978-3-642-38986-3_10 (https://doi.org/10.1007%2F978-3-642-38986-3_10). ISBN 978-3-642-38985-6. S2CID 9135905 (https://api.semanticscholar.org/CorpusID:9135905).

Further reading

- Mingsheng, Ying (2024). *Foundations of quantum programming* (2nd ed.). Cambridge, Massachusetts: Morgan Kaufmann. ISBN 978-0-4431-5942-8. OCLC 1406095194 (https://search.worldcat.org/oclc/1406095194). 978-0-4431-5943-5 (eBook).
- Serrano, Manuel A.; Pérez-Castillo, Ricardo; Piattini, Mario, eds. (2022). *Quantum Software Engineering* (1st ed.). Cham, Switzerland: Springer. doi:10.1007/978-3-031-05324-5 (https://doi.org/10.1007%2F978-3-031-05324-5). ISBN 978-3-031-05323-8. OCLC 1347696597 (https://search.worldcat.org/oclc/1347696597). 978-3-031-05326-9 (softcover) & 978-3-031-05324-5 (eBook).

External links

- Curated list (https://github.com/qosf/awesome-quantum-software) of all quantum open-source software projects
- Bibliography on Quantum Programming Languages (http://www.dcs.gla.ac.uk/~simon/quantum/) (updated in May 2007)
- Quantum Physics and Logic (QPL) Conference Series (https://www.mathstat.dal.ca/~selinger/qpl/) (L stood for 'Languages' until 2006)
- Quantum programming language (https://quantiki.org/wiki/quantum-programming-language) in Quantiki (http://www.quantiki.org/)
- QMASM documentation (https://github.com/lanl/qmasm/wiki)

- pyQuil documentation (https://pyquil.readthedocs.io/en/stable/index.html) including Introduction to Quantum Computing (https://pyquil.readthedocs.io/en/stable/intro.html) Archived (https://web.archive.org/web/20180718165337/https://pyquil.readthedocs.io/en/stable/intro.html) July 18, 2018, at the Wayback Machine
- Scaffold Source (https://github.com/epiqc/ScaffCC)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Quantum_programming&oldid=1241083092"