Quantum computing

A **quantum computer** is a computer that takes advantage of quantum mechanical phenomena.

At small scales, physical matter exhibits properties of both particles and waves, and quantum computing leverages this behavior, specifically quantum superposition and entanglement, using specialized hardware that supports the preparation and manipulation of quantum states.

Classical physics cannot explain the operation of these quantum devices, and a scalable quantum computer could perform some calculations exponentially faster[2] than any modern "classical" computer. In particular, a large-scale quantum computer could break widely used encryption

IBM Q System One, a quantum computer with 20 superconducting qubits[1]

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. Moreover, scalable quantum computers do not hold promise for many practical tasks, and for many important tasks quantum speedups are proven impossible.

The basic unit of information in quantum computing is the qubit, similar to the bit in traditional digital electronics. Unlike a classical bit, 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, therefore making quantum computers nondeterministic in general. 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. Paradoxically, perfectly isolating qubits is also undesirable because quantum computations typically need to initialize qubits, perform controlled qubit interactions, and measure the resulting quantum states. Each of those operations introduces errors and suffers from noise, and such inaccuracies accumulate.

National governments have invested heavily in experimental research that aims to develop scalable qubits with longer coherence times and lower error rates. Two of the most promising technologies are superconductors (which isolate an electrical current by eliminating electrical resistance) and ion traps (which confine a single ion using electromagnetic fields).

In principle, a non-quantum (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 for carefully selected tasks require exponentially fewer computational steps than the best known non-quantum algorithms. Such tasks can in theory be solved on a large-scale quantum computer whereas classical computers would not finish computations in any reasonable amount of time. However, quantum speedup is not universal or even

typical across computational tasks, since basic tasks such as sorting are proven to not allow any asymptotic quantum speedup. Claims of *quantum supremacy* have drawn significant attention to the discipline, but are demonstrated on contrived tasks, while near-term practical use cases remain limited.

Optimism about quantum computing is fueled by a broad range of new theoretical hardware possibilities facilitated by quantum physics, but the improving understanding of quantum computing limitations counterbalances this optimism. In particular, quantum speedups have been traditionally estimated for noiseless quantum computers, whereas the impact of noise and the use of quantum error-correction can undermine low-polynomial speedups.

History

For many years, the fields of quantum mechanics and computer science formed distinct academic communities.[3] Modern quantum theory developed in the 1920s to explain the wave–particle duality observed at atomic scales,[4] and digital computers emerged in the following decades to replace human computers for tedious calculations.[5] Both disciplines had practical applications during World War II; computers played a major role in wartime cryptography,[6] and quantum physics was essential for the nuclear physics used in the Manhattan Project.[7]

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.[8] When digital computers became faster, physicists faced an exponential increase in overhead when simulating quantum dynamics,[9] prompting Yuri Manin and Richard Feynman to independently suggest that hardware based on quantum phenomena might be more efficient for computer simulation.[10][11][12] 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.[13][14]

Quantum algorithms then emerged for solving oracle problems, such as Deutsch's algorithm in 1985,[15] the Bernstein–Vazirani algorithm in 1993,[16] and Simon's algorithm in 1994.[17] 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*.[18] Peter Shor built on these results with his 1994 algorithms for breaking the widely used RSA and Diffie–Hellman encryption protocols,[19] which drew significant attention to the field of quantum computing.[20] In 1996, Grover's algorithm established a quantum speedup for the widely applicable unstructured search problem.[21][22] The same year, Seth Lloyd proved that quantum computers could simulate quantum systems without the exponential overhead present in classical simulations,[23] validating Feynman's 1982 conjecture.[24]

Over the years, experimentalists have constructed small-scale quantum computers using trapped ions and superconductors.[25] In 1998, a two-qubit quantum computer demonstrated the feasibility of the technology,[26][27] and subsequent experiments have increased the number of qubits and reduced error rates.[25] 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.[28][29][30] However, the validity of this claim is still being actively researched.[31][32]

The threshold theorem shows how increasing the number of qubits can mitigate errors,[33] yet fully fault-tolerant quantum computing remains "a rather distant dream".[34] 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.[34]

Investment in quantum computing research has increased in the public and private sectors.[35][36] As one consulting firm summarized,[37]

> ... 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.

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

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.[38]

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,[39]

> 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

The *qubit* serves as the basic unit of quantum information. It represents a two-state system, just like a classical bit, except that it can exist in a *superposition* of its two states.[40] In one sense, a superposition is like a probability distribution over the two values.[41] However, a quantum computation can be influenced by both values at once, inexplicable by either state individually. In this sense, a "superposed" qubit stores both values simultaneously.[18]

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 $\alpha|0\rangle + \beta|1\rangle$, where $|0\rangle$ and $|1\rangle$ are the standard *basis states*,[a] and α and β are the *probability amplitudes*. 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.[41] Negative amplitudes allow for destructive wave interference.[b]

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 $\alpha|0\rangle + \beta|1\rangle$, the state collapses to $|0\rangle$ with probability $|\alpha|^2$, or to $|1\rangle$ 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 $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ would produce either $|0\rangle$ or $|1\rangle$ with equal probability.

Each additional qubit doubles the dimension of the state space. 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

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

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

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

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 (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.
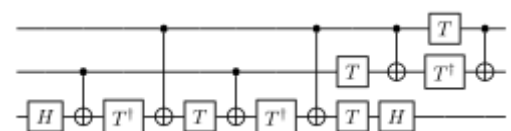
Quantum parallelism

Quantum parallelism refers to the ability of quantum computers to evaluate 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.[18]

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.

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.[43]

Topological quantum computing

A topological quantum computer decomposes computation into the braiding of anyons in a 2D lattice.[44]

Quantum Turing machine

A quantum Turing machine is the quantum analog of a Turing machine.[8] All of these models of computation—quantum circuits,[45] one-way quantum computation,[46] adiabatic quantum computation,[47] and topological quantum computation[48]—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.

Communication

Quantum cryptography enables new ways to transmit data securely; for example, quantum key distribution uses entangled quantum states to establish secure cryptographic keys.[49] 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.[50] With appropriate cryptographic protocols, the sender and receiver can thus establish shared private information resistant to eavesdropping.[13][51]

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.[52][53]

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.[54]

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.[54] 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.[55] 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.[56]

Some quantum algorithms, like Grover's algorithm and amplitude amplification, give polynomial speedups over corresponding classical algorithms.[54] Though these algorithms give comparably modest quadratic speedup, they are widely applicable and thus give speedups for a wide range of problems.[22]

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.[57] Quantum simulation could also be used to simulate the behavior of atoms and particles at unusual conditions such as the reactions inside a collider.[58] In June 2023, IBM computer scientists reported that a quantum computer produced better results for a physics problem than a conventional supercomputer.[59][60]

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.[61] It is expected that an early use of quantum computing will be modeling that improves the efficiency of the Haber–Bosch process[62] by the mid 2020s[63] although some have predicted it will take longer.[64]

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).[65] By comparison, a quantum computer could solve this problem exponentially faster using Shor's algorithm to find its factors.[66] 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*.[67][68] 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.[67][69] 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.[70] 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,[71] 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,[72] and Farhi, Goldstone, and Gutmann's algorithm for evaluating NAND trees.[73]

Problems that can be efficiently addressed with Grover's algorithm have the following properties:[74][75]

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[76] 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.[77]

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.[78]
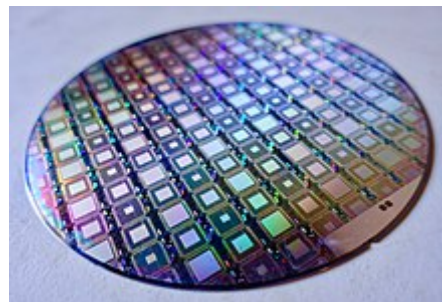
Machine learning

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.[79][34]

For example, the quantum algorithm for linear systems of equations, or "HHL Algorithm", named after its discoverers Harrow, Hassidim, and Lloyd, is believed to provide speedup over classical counterparts.[80][34] Some research groups have recently explored the use of quantum annealing hardware for training Boltzmann machines and deep neural networks.[81][82][83]

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[23] and thus may be instrumental in applications involving quantum chemistry. Therefore, one can expect that quantum-enhanced generative models[84] including quantum GANs[85] 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. For many tasks there is no promise of useful quantum speedup, and some tasks provably prohibit any quantum speedup in the sense that any speedup is ruled out by proved theorems. Scientists and engineers are exploring multiple technologies for quantum computing hardware and hope to develop scalable quantum architectures, but serious obstacles remain.[86][87]

A wafer of adiabatic quantum computers

Challenges

There are a number of technical challenges in building a large-scale quantum computer.[88] Physicist David DiVincenzo has listed these requirements for a practical quantum computer:[89]

- 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.[90]

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.[91]

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.[92] Currently, some quantum computers require their qubits to be cooled to 20 millikelvin (usually using a dilution refrigerator[93]) in order to prevent significant decoherence.[94] A 2020 study argues that ionizing radiation such as cosmic rays can nevertheless cause certain systems to decohere within milliseconds.[95]

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.[96]

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.[97] 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[98][99] 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[100] 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.[101][102]

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.[103][104][105] The problem need not be useful, so some view the quantum supremacy test only as a potential future benchmark.[106]

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.[29][107][108] This claim has been subsequently challenged: IBM has stated that Summit can perform samples much faster than claimed,[109][110] 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[111][112][113] and even beating it.[114][115][116]

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.[117][118][119] 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.[120]

Claims of quantum supremacy have generated hype around quantum computing,[121] but they are based on contrived benchmark tasks that do not directly imply useful real-world applications.[86][122]

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".[86] 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[87] 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 and does not rule out practical simulation on conventional computers, possibly except for contrived cases.
- 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.[123][124] In particular, processing large amounts of non-quantum data is a challenge for quantum computers.[87]
- 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.[87]
- 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 asymptotically 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.[125] Paul Davies argued that a 400-qubit computer would even come into conflict with the cosmological information bound implied by the holographic principle.[126] Skeptics like Gil Kalai doubt that quantum supremacy will ever be achieved.[127][128][129] 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.*"[130][131]

Candidates for physical realizations

A practical quantum computer must use a physical system as a programmable quantum register.[132] Researchers are exploring several technologies as candidates for reliable qubit implementations.[133] Superconductors and trapped ions are some of the most developed proposals, but experimentalists are considering other hardware possibilities as well.[134]

Theory

Computability

Any computational problem solvable by a classical computer is also solvable by a quantum computer.[135] 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.[136]

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.
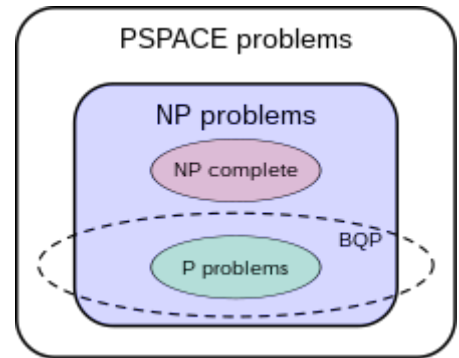
The class of problems that can be efficiently solved by a quantum computer with bounded error is called BQP, for "bounded error, quantum, polynomial time". More formally, BQP is the class of problems that can be solved by a polynomial-time quantum Turing machine with an error probability of at most 1/3. 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.[137] It is known that $BPP \subseteq BQP$ and is widely suspected that $BQP \subsetneq BPP$, which intuitively would mean that quantum computers are more powerful than classical computers in terms of time complexity.[138]

The exact relationship of BQP to P, NP, and PSPACE is not known. However, it is known that $P \subseteq BQP \subseteq PSPACE$; 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 $NP \nsubseteq BQP$; 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).[139]

The suspected relationship of BQP to several classical complexity classes[56]

See also

- D-Wave Systems – Canadian quantum computing company
- Electronic quantum holography
- Glossary of quantum computing
- IARPA
- List of emerging technologies
- List of quantum processors
- Magic state distillation – Quantum computing algorithm
- Natural computing
- Optical computing
- Quantum bus
- Quantum cognition
- Quantum volume
- Quantum weirdness – Unintuitive aspects of quantum mechanics
- Rigetti Computing
- Supercomputer
- Theoretical computer science
- Unconventional computing
- Valleytronics

Notes

a. The standard basis is also the *computational basis*.[42]
b. In general, probability amplitudes are complex numbers.

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. Here and in the following „exponentially faster" has a precise complexity theoretical meaning regarding the potential quantum speedup enabled by quantum computers. Namely, that for certain problems the worst-case time complexity (number of elementary steps needed to solve the problem) of the quantum algorithm scales superpolynomially better than the best known classical algorithm. It thus implies the conjecture that the set of problems efficiently solvable on a quantum computer (BQP) is strictly larger than the set of problems efficiently solvable on a classical computer (BPP). See, for example, Nielsen and Chuang, *Quantum Computation and Quantum Information*, chapter on quantum computational complexity or Scott Aaronson. "How Much Structure Is Needed for Huge Quantum Speedups?" (https://arxiv.org/abs/2209.06930). Edited transcript of a rapporteur talk delivered at the 28th Solvay Physics Conference in Brussels on May 21, 2022. arXiv:2209.06930 (https://arxiv.org/abs/2209.06930).

3. Aaronson 2013, p. 132.

4. Bhatta, Varun S. (10 May 2020). "Plurality of Wave–Particle Duality" (https://wwwops.current science.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%2F136 5-1374). ISSN 0011-3891 (https://www.worldcat.org/issn/0011-3891). S2CID 216143449 (htt ps://api.semanticscholar.org/CorpusID:216143449).

5. Ceruzzi, Paul E. (2012). *Computing: A Concise History*. Cambridge, Massachusetts: MIT Press. pp. 3, 46. ISBN 978-0-262-31038-3. OCLC 796812982 (https://www.worldcat.org/ocl c/796812982).

6. Hodges, Andrew (2014). *Alan Turing: The Enigma*. Princeton, New Jersey: Princeton University Press. p. xviii. ISBN 9780691164724.

7. 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 (http s://ui.adsabs.harvard.edu/abs/2006PhyEd..41..493M). doi:10.1088/0031-9120/41/6/001 (http s://doi.org/10.1088%2F0031-9120%2F41%2F6%2F001). ISSN 0031-9120 (https://www.worl dcat.org/issn/0031-9120). S2CID 120294023 (https://api.semanticscholar.org/CorpusID:120 294023).

8. 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.harva rd.edu/abs/1980JSP....22..563B). doi:10.1007/bf01011339 (https://doi.org/10.1007%2Fbf010 11339). S2CID 122949592 (https://api.semanticscholar.org/CorpusID:122949592).

9. 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..10 8B). doi:10.1126/science.1177838 (https://doi.org/10.1126%2Fscience.1177838). ISSN 0036-8075 (https://www.worldcat.org/issn/0036-8075). PMID 19797653 (https://pubme d.ncbi.nlm.nih.gov/19797653). S2CID 17187000 (https://api.semanticscholar.org/CorpusID:1 7187000).

10. Manin, Yu. I. (1980). *Vychislimoe i nevychislimoe* (https://web.archive.org/web/20130510173 823/http://publ.lib.ru/ARCHIVES/M/MANIN_Yuriy_Ivanovich/Manin_Yu.I._Vychislimoe_i_ne vychislimoe.(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_I vanovich/Manin_Yu.I._Vychislimoe_i_nevychislimoe.(1980).%5bdjv-fax%5d.zip) on 10 May 2013. Retrieved 4 March 2013.

11. Feynman, Richard (June 1982). "Simulating Physics with Computers" (https://web.archive.or g/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 (htt ps://api.semanticscholar.org/CorpusID:124545445). Archived from the original (https://peopl e.eecs.berkeley.edu/~christos/classics/Feynman.pdf) (PDF) on 8 January 2019. Retrieved 28 February 2019.

12. Nielsen & Chuang 2010, p. 214.

13. Bennett, Charles H.; Brassard, Gilles (December 1984). *Quantum cryptography: Public key distribution and coin tossing*. IEEE International Conference on Computers, Systems & Signal Processing. Bangalore. pp. 175–179. arXiv:2003.06557 (https://arxiv.org/abs/2003.06 557). doi:10.1016/j.tcs.2014.05.025 (https://doi.org/10.1016%2Fj.tcs.2014.05.025).

14. Brassard, G. (2005). "Brief history of quantum cryptography: A personal perspective" (https://i eeexplore.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:1611 8245).

15. 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.h arvard.edu/abs/1985RSPSA.400...97D). doi:10.1098/rspa.1985.0070 (https://doi.org/10.109 8%2Frspa.1985.0070). ISSN 0080-4630 (https://www.worldcat.org/issn/0080-4630). S2CID 1438116 (https://api.semanticscholar.org/CorpusID:1438116).

16. Bernstein, Ethan; Vazirani, Umesh (1993). "Quantum complexity theory" (http://portal.acm.or g/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:67637 8).

17. Simon, D. R. (1994). "On the power of quantum computation" (https://ieeexplore.ieee.org/doc ument/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:74578 14).

18. Nielsen & Chuang 2010, p. 30-32.

19. Shor 1994.

20. National Academies of Sciences, Engineering, and Medicine 2019, p. 15.

21. 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://do i.org/10.1145%2F237814.237866). ISBN 978-0-89791-785-8.

22. Nielsen & Chuang 2010, p. 7.

23. 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://www.worldcat.org/issn/0036-8075). PMID 8688088 (https://pubmed.ncbi.nlm.nih.gov/8688088). S2CID 43496899 (https://api.semanticscholar.org/CorpusID:43496899).

24. 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://www.worldcat.org/issn/0009-2665). PMID 31469277 (https://pubmed.ncbi.nlm.nih.gov/31469277). S2CID 119417908 (https://api.semanticscholar.org/CorpusID:119417908).

25. National Academies of Sciences, Engineering, and Medicine 2019, pp. 164–169.

26. Chuang, Isaac L.; Gershenfeld, Neil; Kubinec, Markdoi (April 1998). "Experimental Implementation of Fast Quantum Searching". *Physical Review Letters*. American Physical Society. **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).

27. Holton, William Coffeen. "quantum computer" (https://www.britannica.com/technology/quantum-computer). *Encyclopedia Britannica*. Encyclopædia Britannica. Retrieved 4 December 2021.

28. 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).

29. 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*. Google AI. **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). 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).

30. 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://www.worldcat.org/issn/0362-4331). Retrieved 25 September 2021.

31. 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.

32. 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)].

33. Nielsen & Chuang 2010, p. 481.

34. 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).

35. 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).

36. 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.

37. 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.

38. 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.

39. 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.

40. Nielsen & Chuang 2010, p. 13.

41. Aaronson 2013, p. 110.

42. Mermin 2007, p. 18.

43. 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).

44. 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).

45. 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).

46. 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..68b2312 R). doi:10.1103/PhysRevA.68.022312 (https://doi.org/10.1103%2FPhysRevA.68.022312). S2CID 6197709 (https://api.semanticscholar.org/CorpusID:6197709).

47. 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/2008 SIAMR..50..755A). doi:10.1137/080734479 (https://doi.org/10.1137%2F080734479). ISSN 0036-1445 (https://www.worldcat.org/issn/0036-1445). S2CID 1503123 (https://api.se manticscholar.org/CorpusID:1503123).

48. 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/000110 8). Bibcode:2002CMaPh.227..605F (https://ui.adsabs.harvard.edu/abs/2002CMaPh.227..60 5F). doi:10.1007/s002200200645 (https://doi.org/10.1007%2Fs002200200645). ISSN 0010-3616 (https://www.worldcat.org/issn/0010-3616). S2CID 8990600 (https://api.semanticschola r.org/CorpusID:8990600).

49. 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/190 6.01645). 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://www.worldcat.org/issn/1943-8206). S2CID 174799187 (https://api.semanticsch olar.org/CorpusID:174799187).

50. 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).

51. 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%2FCISS5650 2.2023.10089619). ISBN 978-1-6654-5181-9.

52. 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.or g/abs/1909.08396). doi:10.1145/3345312.3345497 (https://doi.org/10.1145%2F3345312.33 45497). ISBN 978-1-4503-6897-1.

53. 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/1905.094 08). doi:10.1038/s41567-019-0743-x (https://doi.org/10.1038%2Fs41567-019-0743-x). ISSN 1745-2473 (https://www.worldcat.org/issn/1745-2473). S2CID 256703226 (https://api.s emanticscholar.org/CorpusID:256703226).

54. 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.

55. 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.

56. Nielsen & Chuang 2010, p. 42.

57. Norton, Quinn (15 February 2007). "The Father of Quantum Computing" (http://archive.wired.com/science/discoveries/news/2007/02/72734). *Wired*.

58. 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.

59. 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.

60. 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).

61. Morello, Andrea (21 November 2018). *Lunch & Learn: Quantum Computing* (https://www.youtube.com/watch?v=7susESgnDv8). Sibos TV. Archived (https://ghostarchive.org/varchive/youtube/20211211/7susESgnDv8) from the original on 11 December 2021. Retrieved 4 February 2021 – via YouTube.

62. 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://www.worldcat.org/issn/0017-8012). Retrieved 12 April 2023.

63. 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.

64. 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.

65. 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.

66. Nielsen & Chuang 2010, p. 216.

67. 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).

68. 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.

69. 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).

70. 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).

71. 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).

72. 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).

73. 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://www.worldcat.org/issn/1557-2862). S2CID 8258191 (https://api.semanticscholar.org/CorpusID:8258191).

74. Williams, Colin P. (2011). *Explorations in Quantum Computing*. Springer. pp. 242–244. ISBN 978-1-84628-887-6.

75. Grover, Lov (29 May 1996). "A fast quantum mechanical algorithm for database search". arXiv:quant-ph/9605043 (https://arxiv.org/abs/quant-ph/9605043).

76. 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).

77. 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*.

78. 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).

79. 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://www.worldcat.org/issn/0028-0836). PMID 28905917 (https://pubmed.ncbi.nlm.nih.gov/28905917). S2CID 64536201 (https://api.semanticscholar.org/CorpusID:64536201).

80. 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).

81. 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).

82. 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://www.worldcat.org/issn/0098-1354). S2CID 211678230 (https://api.semanticscholar.org/CorpusID:211678230).

83. 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. doi:10.1016/j.apenergy.2021.117628 (https://doi.org/10.1016%2Fj.apenergy.2021.117628). ISSN 0306-2619 (https://www.worldcat.org/issn/0306-2619).

84. 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).

85. 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)].

86. 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).

87. 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.

88. Dyakonov, Mikhail (15 November 2018). "The Case Against Quantum Computing" (https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing). *IEEE Spectrum*.

89. 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).

90. 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.

91. 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).

92. 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).

93. 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://www.worldcat.org/issn/0011-2275). S2CID 244005391 (https://api.semanticscholar.org/CorpusID:244005391).

94. 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).

95. 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://www.worldcat.org/issn/1476-4687). PMID 32848227 (https://pubmed.ncbi.nlm.nih.gov/32848227). S2CID 210920566 (https://api.semanticscholar.org/CorpusID:210920566).

96. 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)].

97. 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).

98. Ahsan, Muhammad (2015). *Architecture Framework for Trapped-ion Quantum Computer based on Performance Simulation Tool* (http://worldcat.org/oclc/923881411). OCLC 923881411 (https://www.worldcat.org/oclc/923881411).

99. 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. doi:10.1145/2830570 (https://doi.org/10.1145%2F2830570). ISSN 1550-4832 (https://www.worldcat.org/issn/1550-4832). S2CID 1258374 (https://api.semanticscholar.org/CorpusID:1258374).

100. 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://www.worldcat.org/issn/2521-327X). S2CID 162183806 (https://api.semanticscholar.org/CorpusID:162183806).

101. 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).

102. 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*.

103. 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)].

104. 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).

105. 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).

106. Savage, Neil (5 July 2017). "Quantum Computers Compete for "Supremacy" " (https://www.scientificamerican.com/article/quantum-computers-compete-for-supremacy/). *Scientific American*.

107. 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.

108. Tavares, Frank (23 October 2019). "Google and NASA Achieve Quantum Supremacy" (http://www.nasa.gov/feature/ames/quantum-supremacy). *NASA*. Retrieved 16 November 2021.

109. 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)].

110. 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://www.worldcat.org/issn/0036-8075). S2CID 211982610 (https://api.semanticscholar.org/CorpusID:211982610).

111. 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).

112. 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://www.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).

113. 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).

114. 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).

115. 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).

116. "Google's 'quantum supremacy' usurped by researchers using ordinary supercomputer" (https://social.techcrunch.com/2022/08/05/googles-quantum-supremacy-usurped-by-researchers-using-ordinary-supercomputer/). *TechCrunch*. 5 August 2022. Retrieved 7 August 2022.

117. 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).

118. 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.

119. 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.

120. 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://www.worldcat.org/issn/0036-8075). PMID 33273064 (https://pubmed.ncbi.nlm.nih.gov/33273064). S2CID 227254333 (https://api.semanticscholar.org/CorpusID:227254333).

121. 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://www.worldcat.org/issn/0963-6625). PMID 32438851 (https://pubmed.ncbi.nlm.nih.gov/32438851). S2CID 218831653 (https://api.semanticscholar.org/CorpusID:218831653).

122. 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://www.worldcat.org/issn/1353-4858). S2CID 222349414 (https://api.semanticscholar.org/CorpusID:222349414).

123. 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.

124. 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*.

125. 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).

126. 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).

127. 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*.

128. 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.

129. 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)].

130. Dyakonov, Mikhail (15 November 2018). "The Case Against Quantum Computing" (https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing). *IEEE Spectrum*. Retrieved 3 December 2019.

131. 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.

132. 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://www.worldcat.org/issn/2511-9044). S2CID 195833616 (https://api.semanticscholar.org/CorpusID:195833616).

133. National Academies of Sciences, Engineering, and Medicine 2019, p. 127.

134. National Academies of Sciences, Engineering, and Medicine 2019, p. 114.

135. Nielsen & Chuang 2010, p. 29.

136. Nielsen & Chuang 2010, p. 126.

137. Nielsen & Chuang 2010, p. 41.

138. Nielsen & Chuang 2010, p. 201.

139. 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).

Further reading

Textbooks

- 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://www.worldcat.org/oclc/829706638).

- 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://www.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://www.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://www.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://www.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://www.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://www.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://www.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://www.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://www.worldcat.org/oclc/907358694).
- 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://www.worldcat.org/oclc/422727925).
- 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://www.worldcat.org/oclc/1091904777). S2CID 125635007 (https://api.semanticscholar.org/CorpusID:125635007).
- 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://www.worldcat.org/oclc/700706156). S2CID 59717455 (https://api.semanticscholar.org/CorpusID:59717455).
- 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://www.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://www.worldcat.org/oclc/1178715016). S2CID 225498497 (https://api.semanticscholar.org/CorpusID:225498497).
- Wong, Thomas (2022). *Introduction to Classical and Quantum Computing* (http://www.thomaswong.net/introduction-to-classical-and-quantum-computing-1e.pdf) (PDF). Rooted Grove. ISBN 979-8-9855931-0-5. OCLC 1308951401 (https://www.worldcat.org/oclc/1308951401).
- 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://www.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). 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://www.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).

- 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.

- 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)

-