

Introduction to Quantum Mechanics And Quantum Computing

Natansh N

natanshmom2003@gmail.com

Quantum Mechanics Basics

Quantum mechanics is the study of matter and its interactions with energy on the scale of atomic and subatomic particles. By contrast, classical physics explains matter and energy only on a scale familiar to human experience, including the behaviour of astronomical bodies such as the moon. Classical physics is still used in much of modern science and technology. However, towards the end of the 19th century, scientists discovered phenomena in both the large (macro) and the small (micro) worlds that classical physics could not explain. The desire to resolve inconsistencies between observed phenomena and classical theory led to a revolution in physics, a shift in the original scientific paradigm the development of quantum mechanics.

Many aspects of quantum mechanics are counterintuitive and can seem paradoxical because they describe behaviour quite different from that seen at larger scales. In the words of quantum physicist Richard Feynman, quantum mechanics deals with "nature as She is—absurd".

One example of this is the uncertainty principle applied to particles, which implies that the more closely one pins down one measurement on a particle (such as the position of an electron), the less accurate another complementary measurement pertaining to the same particle (such as its speed) must become. The position and speed of a particle cannot both be measured with arbitrary precision, regardless of the quality of the measuring instruments.

Another example is entanglement. In certain circumstances, two particles with a shared history may become mutually 'entangled', in which case a measurement made on one particle (such as an electron that is measured to have spin up) will provide full information about the outcome of a later equivalent measurement on the other particle (that the other will be found to have spin down). This applies even though the particles may be so far apart that it is impossible for the result of the first measurement to have been transmitted to the second particle before the second measurement takes place.

A further example is superfluidity. Liquid helium in a container, cooled to a temperature near absolute zero spontaneously flows up and over the rim of its container, an effect which cannot be explained by classical physics.

History

Maxwell's unification of electricity, magnetism, and even light in the 1880s led to experiments on the interaction of light and matter. Some of these experiments had aspects which could not be explained. Quantum mechanics emerged in the early part of the 20th century from efforts to explain these results.

Evidence of quanta from the photo electric effect

The seeds of the quantum revolution appear in the discovery by JJ Thomson in 1897 that cathode rays were not continuous but "corpuscles" now called electrons. Electrons had been named just six years earlier as part of the emerging theory of atoms. In 1900, Max Planck, a conservative physicist unconvinced by the atomic theory, discovered that he needed discrete entities like atoms or electrons to explain blackbody radiation.

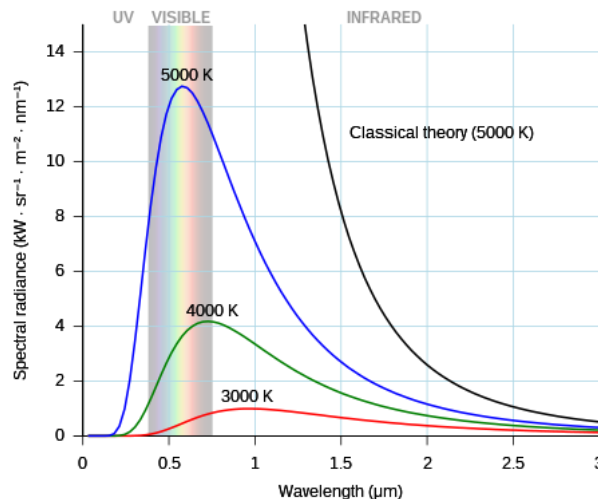


Fig.1: Blackbody radiation intensity vs colour and temperature. The rainbow bar represents visible light; 5000K objects are "white hot" by mixing differing colours of visible light. To the right is the invisible infrared. Classical theory (black curve for 5000K) fails; the other curves are correct predicted by quantum theories.

Hot objects radiate heat; very hot objects – red hot, white hot objects – all look similar when heated to the same temperature. This temperature dependent "look" results from a common curve of light intensity at different frequencies (colours). The common curve is called blackbody radiation. The lowest frequencies are invisible heat rays – infrared light. White hot objects have intensity across many colours in the visible range. Continuous wave theories of light and matter cannot explain the blackbody radiation curve. Planck spread the heat energy among individual "oscillators" of an undefined character but with discrete energy capacity: the blackbody radiation behaviour was then predicted by this model.

At the time, electrons, atoms, and discrete oscillators were all exotic ideas to explain exotic phenomena. But in 1905 Albert Einstein proposed that light was also corpuscular, consisting of "energy quanta", seemingly in contradiction to the established science of light as a continuous wave, stretching back a hundred years to Thomas Young's work on diffraction.

His revolutionary proposal started by reanalysing Planck blackbody theory, arriving at the same conclusions by using the new "energy quanta". Einstein then showed how energy quanta connected to JJ Thomson's electron. In 1902, Philipp Lenard directed light from an arc lamp onto freshly cleaned metal plates housed in an evacuated glass tube. He measured the electric current coming off the metal plate, for higher and lower intensity of light and for different metals. This is the photoelectric effect. Lenard showed that amount of current – the number of electrons – depended on the intensity of the light, but that the velocity of these electrons did not depend on intensity. The continuous wave theories of the time would predict that more light intensity would accelerate the same amount of current to higher velocity contrary to experiment. Einstein's energy quanta explained the volume increase: one electron is ejected for each quanta: more quanta mean more electrons.

Einstein then predicted that the electron velocity would increase in direct proportion to the light frequency above a fixed value that depended upon the metal. Here the idea is that energy in energy-quanta depends upon the light frequency; the energy transferred to the electron comes in proportion to the light frequency. The type of metal gives a barrier, the fixed value, that the electrons must climb over to exit their atoms, to be emitted from the metal surface and be measured. Ten years elapsed before Millikan's definitive experiment verified Einstein's prediction. During that time many scientists rejected the revolutionary idea of quanta. But Planck's and Einstein's concept was in the air and soon affected other theories.

Quantization of bound electrons in atoms

Experiments with light and matter in the late 1800s uncovered a reproducible but puzzling regularity. When light was shown through purified gasses, certain frequencies (colours) did not pass. These dark absorption 'lines' followed a distinctive pattern: the gaps between the lines decreased steadily. By 1889, the Rydberg formula predicted the lines for hydrogen gas using only a constant number and the integers to index the lines. The origin of this regularity was unknown. Solving this mystery would become first major step toward quantum mechanics.

Throughout the 19th century evidence grew for the atomic nature of matter. With JJ Thomson's discovery of the electron in 1897, scientist began the search for a model of the interior of the atom. Thomson proposed negative electrons swimming in a pool of positive charge. Between 1908 and 1911, Rutherford showed that the positive part was only 1/3000th of the diameter of the atom.

Models of "planetary" electrons orbiting a nuclear "Sun" were proposed, but cannot explain why the electron does not simply fall into the positive charge. In 1913 Neils Bohr and Ernest Rutherford connected the new atom models to the mystery of the Rydberg formula: the orbital radius of the electrons were constrained and the resulting energy differences matched the energy differences in the absorption lines. This meant that absorption and emission of light from atoms was energy quantized: only specific energies that matched the difference in orbital energy would be emitted or absorbed.

Trading one mystery – the regular pattern of the Rydberg formula – for another mystery – constraints on electron orbits – might not seem like a big advance, but the new atom model summarized many other experimental findings. The quantization of the photoelectric effect and now the quantization of the electron orbits set the stage for the final revolution.

Quantization of matter

In 1922 Otto Stern and Walther Gerlach demonstrated that the magnetic properties of silver atoms do not take a continuous range of values: the magnetic values are quantized and limited to only two possibilities. Unlike the other then known quantum effects, this striking result involves the state of a single atom.

In 1924 Louis de Broglie proposed that electrons in an atom are constrained not in "orbits" but as standing waves. In detail his solution did not work, but his hypothesis – that the electron "corpuscle" moves in the atom as a wave – spurred Erwin Schrödinger to develop a wave equation for electrons; when applied to hydrogen the Rydberg formula was accurately reproduced.

Max Born's 1924 paper "*Zur Quantenmechanik*" was the first use of the words "quantum mechanics" in print. His later work included developing quantum collision models; in a footnote to a 1926 paper he proposed the Born rule connecting theoretical models to experiment.

In 1928 Paul Dirac published his relativistic wave equation simultaneously incorporating relativity, predicting anti-matter, and providing a complete theory for the Stern-Gerlach result (that there are only two directions that can be measured for silver atoms and for electrons themselves). These successes launched a new fundamental understanding of our world at small scale: quantum mechanics.

Planck and Einstein started the revolution with quanta that broke down the continuous models of matter and light. Twenty years later "corpuscles" like electrons came to be modelled as continuous waves. This result came to be called wave-particle duality, one iconic idea along with the uncertainty principle that sets quantum mechanics apart from older models of physics.

Quantum radiation, quantum fields

In 1923 Compton demonstrated that the Planck-Einstein energy quanta from light also had momentum; three years later the "energy quanta" got a new name "photon" Despite its role in almost all stages of the quantum revolution, no explicit model for light quanta existed until 1927 when Paul Dirac began work on a quantum theory of radiation that became quantum electrodynamics. Over the following decades this work evolved into quantum field theory, the basis for modern quantum optics and particle physics.

Correspondence principle

Throughout the first and the modern era of quantum mechanics the concept that classical mechanics must be valid macroscopically constrained possible quantum models. This concept was formalized by Bohr in 1923 as the correspondence principle. It requires quantum theory to converge to classical limits.

One principal "paradox" is the apparent inconsistency between Newton's laws and quantum mechanics which can be explained using Ehrenfest's theorem, which shows that the average values obtained from quantum mechanics (e.g. position and momentum) obey classical laws. However, Ehrenfest's theorem is far from capable of explaining all the counterintuitive phenomena (quantum weirdness) that have been observed, but rather is a mathematical expression of the correspondence principle.

Wave-particle duality

The concept of wave-particle duality says that neither the classical concept of "particle" nor of "wave" can fully describe the behavior of quantum-scale objects, either photons or matter. Wave-particle duality is an example of the principle of complementarity in quantum physics. An elegant example of wave-particle duality is the double-slit experiment.

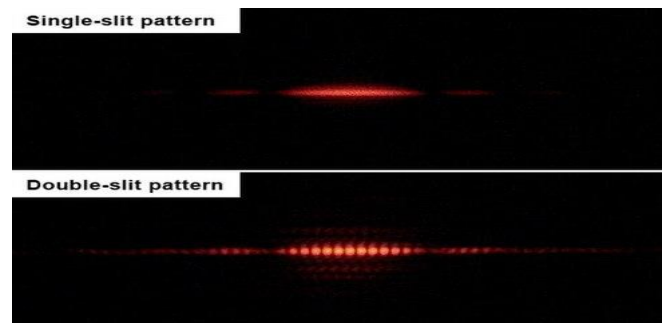


Fig.2: The diffraction pattern produced when light is shone through one slit (top) and the interference pattern produced by two slits (bottom). Both patterns show oscillations due to the wave nature of light. The double slit pattern is more dramatic.

In the double-slit experiment, as originally performed by Thomas Young in 1803, and then Augustin Fresnel a decade later, a beam of light is directed through two narrow, closely spaced slits, producing an interference pattern of light and dark bands on a screen. If one of the slits is covered up, one might naïvely expect that the intensity of the fringes due to interference would be halved everywhere. In fact, a much simpler pattern is seen, a diffraction pattern diametrically opposite the open slit. The same behavior can be demonstrated in water waves, and so the double-slit experiment was seen as a demonstration of the wave nature of light.

Variations of the double-slit experiment have been performed using electrons, atoms, and even large molecules, and the same type of interference pattern is seen. Thus it has been demonstrated that all matter possesses both particle and wave characteristics.

Even if the source intensity is turned down, so that only one particle (e.g. photon or electron) is passing through the apparatus at a time, the same interference pattern develops over time. The quantum particle acts as a wave when passing through the double slits, but as a particle when it is detected. This is a typical feature of quantum complementarity: a quantum particle acts as a wave in an experiment to measure its wave-like properties, and like a particle in an experiment to measure its particle-like properties. The point on the detector screen where any individual particle shows up is the result of a random process. However, the distribution pattern of many individual particles mimics the diffraction pattern produced by waves.

Uncertainty principle

Suppose it is desired to measure the position and speed of an object—for example, a car going through a radar speed trap. It can be assumed that the car has a definite position and speed at a particular moment in time. How accurately these values can be measured depends on the quality of the measuring equipment. If the precision of the measuring equipment is improved, it provides a result closer to the true value. It might be assumed that the speed of the car and its position could be operationally defined and measured simultaneously, as precisely as might be desired.

In 1927, Heisenberg proved that this last assumption is not correct. Quantum mechanics shows that certain pairs of physical properties, for example, position and speed, cannot be simultaneously measured, nor defined in operational terms, to arbitrary precision: the more precisely one property is measured, or defined in operational terms, the less precisely can the other. This statement is known as the uncertainty principle. The uncertainty principle is not only a statement about the accuracy of our measuring equipment but, more deeply, is about the conceptual nature of the measured quantities—the assumption that the car had simultaneously defined position and speed does not work in quantum mechanics. On a scale of cars and people, these uncertainties are negligible, but when dealing with atoms and electrons they become critical.

Heisenberg gave, as an illustration, the measurement of the position and momentum of an electron using a photon of light. In measuring the electron's position, the higher the frequency of the photon, the more accurate is the measurement of the position of the impact of the photon with the electron, but the greater is the disturbance of the electron. This is because from the impact with the photon, the electron absorbs a random amount of energy, rendering the measurement obtained of its momentum increasingly uncertain, for one is necessarily measuring its post-impact disturbed momentum from the collision products and not its original momentum (momentum which should be simultaneously measured with position). With a

photon of lower frequency, the disturbance (and hence uncertainty) in the momentum is less, but so is the accuracy of the measurement of the position of the impact.

At the heart of the uncertainty principle is a fact that for any mathematical analysis in the position and velocity domains, achieving a sharper (more precise) curve in the position domain can only be done at the expense of a more gradual (less precise) curve in the speed domain, and vice versa. More sharpness in the position domain requires contributions from more frequencies in the speed domain to create the narrower curve, and vice versa. It is a fundamental tradeoff inherent in any such related or complementary measurements, but is only really noticeable at the smallest (Planck) scale, near the size of elementary particles.

The uncertainty principle shows mathematically that the product of the uncertainty in the position and momentum of a particle (momentum is velocity multiplied by mass) could never be less than a certain value, and that this value is related to Planck's constant.

Wave function collapse

Wave function collapse means that a measurement has forced or converted a quantum (probabilistic or potential) state into a definite measured value. This phenomenon is only seen in quantum mechanics rather than classical mechanics.

For example, before a photon actually "shows up" on a detection screen it can be described only with a set of probabilities for where it might show up. When it does appear, for instance in the CCD of an electronic camera, the time and space where it interacted with the device are known within very tight limits. However, the photon has disappeared in the process of being captured (measured), and its quantum wave function has disappeared with it. In its place, some macroscopic physical change in the detection screen has appeared, e.g., an exposed spot in a sheet of photographic film, or a change in electric potential in some cell of a CCD.

Eigenstates and eigenvalues

Because of the uncertainty principle, statements about both the position and momentum of particles can assign only a probability that the position or momentum has some numerical value. Therefore, it is necessary to formulate clearly the difference between the state of something indeterminate, such as an electron in a probability cloud, and the state of something having a definite value. When an object can definitely be "pinned-down" in some respect, it is said to possess an eigenstate.

In the Stern–Gerlach experiment discussed above, the spin of the atom about the vertical axis has two eigenstates: up and down. Before measuring it, we can only say that any individual atom has an equal probability of being found to have spin up or spin down. The measurement process causes the wave function to collapse into one of the two states.

The eigenstates of spin about the vertical axis are not simultaneously eigenstates of spin about the horizontal axis, so this atom has an equal probability of being found to have either value of spin about the horizontal axis. As described in the section above, measuring the spin about the horizontal axis can allow an atom that was spun up to spin down: measuring its spin about the horizontal axis collapses its wave function into one of the eigenstates of this measurement, which means it is no longer in an eigenstate of spin about the vertical axis, so can take either value.

Quantum entanglement

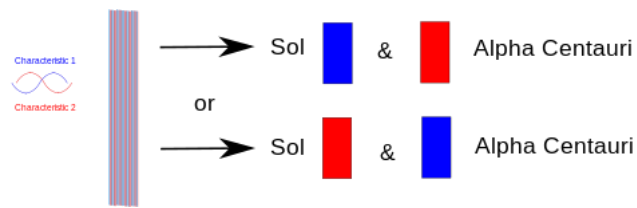


Fig.3: Superposition of two quantum characteristics, and two resolution possibilities

The Pauli exclusion principle says that two electrons in one system cannot be in the same state. Nature leaves open the possibility, however, that two electrons can have both states "superimposed" over each of them. Recall that the wave functions that emerge simultaneously from the double slits arrive at the detection screen in a state of superposition. Nothing is certain until the superimposed waveforms "collapse". At that instant, an electron shows up somewhere in accordance with the probability that is the square of the absolute value of the sum of the complex-valued amplitudes of the two superimposed waveforms. The situation there is already very abstract. A concrete way of thinking about entangled photons, photons in which two contrary states are superimposed on each of them in the same event, is as follows:

Imagine that we have two color-coded states of photons: one state labeled *blue* and another state labeled *red*. Let the superposition of the red and the blue state appear (in imagination) as a *purple* state. We consider a case in which two photons are produced as the result of one single atomic event. Perhaps they are produced by the excitation of a crystal that characteristically absorbs a photon of a certain frequency and emits two photons of half the original frequency. In this case, the photons are interconnected via their shared origin in a single atomic event. This setup results in superimposed states of the photons. So the two photons come out *purple*. If the experimenter now performs some experiment that determines whether one of the photons is either *blue* or *red*, then that experiment changes the photon involved from one having a superposition of *blue* and *red* characteristics to a photon that has only one of those characteristics. The problem that Einstein had with such an imagined situation was that if one of these photons had been kept bouncing between mirrors in a laboratory on earth, and the other one had traveled halfway to the nearest star when its twin was made to reveal itself as either blue or red, that meant that the distant photon now had to lose its *purple* status too. So whenever it might be investigated after its twin had been measured, it would necessarily show up in the opposite state to whatever its twin had revealed.

In trying to show that quantum mechanics was not a complete theory, Einstein started with the theory's prediction that two or more particles that have interacted in the past can appear strongly correlated when their various properties are later measured. He sought to explain this seeming interaction classically, through their common past, and preferably not by some "spooky action at a distance". The argument is worked out in a famous paper, Einstein, Podolsky, and Rosen (1935; abbreviated EPR) setting out what is now called the EPR paradox. Assuming what is now usually called local realism, EPR attempted to show from quantum theory that a particle has both position and momentum simultaneously, while according to the Copenhagen interpretation, only one of those two properties actually exists and only at the moment that it is being measured. EPR concluded that quantum theory is incomplete in that it refuses to consider physical properties that objectively exist in nature. (Einstein, Podolsky, & Rosen 1935 is currently Einstein's most cited publication in physics journals.) In the same year, Erwin Schrödinger used the word "entanglement" and declared: "I would not call that *one* but

rather *the* characteristic trait of quantum mechanics." Ever since Irish physicist John Stewart Bell theoretically and experimentally disproved the "hidden variables" theory of Einstein, Podolsky, and Rosen, most physicists have accepted entanglement as a real phenomenon. However, there is some minority dispute. The Bell inequalities are the most powerful challenge to Einstein's claims.

Interpretations

The physical measurements, equations, and predictions pertinent to quantum mechanics are all consistent and hold a very high level of confirmation. However, the question of what these abstract models say about the underlying nature of the real world has received competing answers. These interpretations are widely varying and sometimes somewhat abstract. For instance, the Copenhagen interpretation states that before a measurement, statements about a particle's properties are completely meaningless, while in the many-worlds interpretation describes the existence of a multiverse made up of every possible universe.

Measurement in quantum mechanics

In quantum physics, a **measurement** is the testing or manipulation of a physical system to yield a numerical result. A fundamental feature of quantum theory is that the predictions it makes are probabilistic. The procedure for finding a probability involves combining a quantum state, which mathematically describes a quantum system, with a mathematical representation of the measurement to be performed on that system. The formula for this calculation is known as the Born rule. For example, a quantum particle like an electron can be described by a quantum state that associates to each point in space a complex number called a probability amplitude. Applying the Born rule to these amplitudes gives the probabilities that the electron will be found in one region or another when an experiment is performed to locate it. This is the best the theory can do; it cannot say for certain where the electron will be found. The same quantum state can also be used to make a prediction of how the electron will be *moving*, if an experiment is performed to measure its momentum instead of its position. The uncertainty principle implies that, whatever the quantum state, the range of predictions for the electron's position and the range of predictions for its momentum cannot both be narrow. Some quantum states imply a near-certain prediction of the result of a position measurement, but the result of a momentum measurement will be highly unpredictable, and vice versa. Furthermore, the fact that nature violates the statistical conditions known as Bell inequalities indicates that the unpredictability of quantum measurement results cannot be explained away as due to ignorance about "hidden variables" within quantum systems.

Measuring a quantum system generally changes the quantum state that describes that system. This is a central feature of quantum mechanics, one that is both mathematically intricate and conceptually subtle. The mathematical tools for making predictions about what measurement outcomes may occur, and how quantum states can change, were developed during the 20th century and make use of linear algebra and functional analysis. Quantum physics has proven to be an empirical success and to have wide-ranging applicability. However, on a more philosophical level, debates continue about the meaning of the measurement concept.

The Birth of Quantum Computing

A **quantum computer** is a computer that exploits quantum mechanical phenomena. At small scales, physical matter exhibits properties of both particles and waves, and quantum computing leverages this behaviour using specialized hardware. Classical physics cannot explain the operation of these quantum devices, and a scalable quantum computer could perform some calculations exponentially faster than any modern "classical" computer. In particular, a large-scale quantum computer could break widely used encryption schemes and aid physicists in

performing physical simulations; however, the current state of the art is largely experimental and impractical, with several obstacles to useful applications.

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. If a quantum computer manipulates the qubit in a particular way, wave interference effects can amplify the desired measurement results. The design of quantum algorithms involves creating procedures that allow a quantum computer to perform calculations efficiently and quickly.

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

In principle, a 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 fuelled 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.

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

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

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

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

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

Quantum Bits (Qubits)

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

Bit versus qubit

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

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

There are two possible outcomes for the measurement of a qubit—usually taken to have the value "0" and "1", like a bit or binary digit. However, whereas the state of a bit can only be

either 0 or 1, the general state of a qubit according to quantum mechanics can be a coherent superposition of both. Moreover, whereas a measurement of a classical bit would not disturb its state, a measurement of a qubit would destroy its coherence and irrevocably disturb the superposition state. It is possible to fully encode one bit in one qubit. However, a qubit can hold more information, e.g., up to two bits using superdense coding.

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

Standard representation

In quantum mechanics, the general quantum state of a qubit can be represented by a linear superposition of its two orthonormal basis states (or basis vectors). These vectors are usually denoted as $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. They are written in the conventional Dirac—or "bra-ket"—notation; the $|0\rangle$ and $|1\rangle$ are pronounced "ket 0" and "ket 1", respectively. These two orthonormal basis states, $\{|0\rangle, |1\rangle\}$, together called the computational basis, are said to span the two-dimensional linear vector (Hilbert) space of the qubit. Qubit basis states can also be combined to form product basis states. A set of qubits taken together is called a quantum register. For example, two qubits could be represented in a four-dimensional linear vector space

spanned by the following product basis states: $|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, $|01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$, $|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$,
 and $|11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$.

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

Qubit states

A pure qubit state is a coherent superposition of the basis states. This means that a single qubit

(ψ) can be described by a linear combination of $|0\rangle$ and $|1\rangle$: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

where α and β are the probability amplitudes, and are both complex numbers. When we measure this qubit in the standard basis, according to the Born rule, the probability of outcome $|0\rangle$ with value "0" is $|\alpha|^2$ and the probability of outcome $|1\rangle$ with value "1" is $|\beta|^2$. Because the absolute squares of the amplitudes equate to probabilities, it follows that α and β must be constrained according to the second axiom of probability theory by the equation $|\alpha|^2 + |\beta|^2 = 1$. The probability amplitudes, α and β , encode more than just the probabilities of the outcomes of a measurement; the *relative phase* between α and β is for example responsible for quantum interference, as seen in the two-slit experiment.

Operations on qubits

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

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

Quantum Entanglement

An important distinguishing feature between qubits and classical bits is that multiple qubits can exhibit quantum entanglement. Quantum entanglement is a nonlocal property of two or more qubits that allows a set of qubits to express higher correlation than is possible in classical systems.

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

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

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

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

value “0” or “1” — a most surprising circumstance that can not be explained by classical physics.

Quantum Gates and Circuits

In quantum computing and specifically the quantum circuit model of computation, a quantum logic gate is a basic quantum circuit operating on a small number of qubits. They are the building blocks of quantum circuits, like classical logic gates are for conventional digital circuits.

Unlike many classical logic gates, quantum logic gates are reversible. It is possible to perform classical computing using only reversible gates. For example, the reversible Toffoli gate can implement all Boolean functions, often at the cost of having to use ancilla bits. The Toffoli gate has a direct quantum equivalent, showing that quantum circuits can perform all operations performed by classical circuits.

Quantum gates are unitary operators, and are described as unitary matrices relative to some basis. Usually the *computational basis* is used, which unless comparing it with something, just means that for a d -level quantum system (such as a qubit, a quantum register, or qutrits and qubits) the orthogonal basis vectors are labelled $|0\rangle, |1\rangle, \dots, |d-1\rangle$, or use binary notation.

Representation

Quantum logic gates are represented by unitary matrices. A gate which acts on n qubits is represented by a $2^n \times 2^n$ unitary matrix, and the set of all such gates with the group operation of matrix multiplication^[a] is the symmetry group $U(2^n)$. The quantum states that the gates act upon are unit vectors in n complex dimensions, with the complex Euclidean norm (the 2-norm). The basis vectors (sometimes called *eigenstates*) are the possible outcomes if measured, and a quantum state is a linear combination of these outcomes. The most common quantum gates operate on vector spaces of one or two qubits, just like the common classical logic gates operate on one or two bits.

Even though the quantum logic gates belong to continuous symmetry groups, real hardware is inexact and thus limited in precision. The application of gates typically introduces errors, and the quantum states fidelities decreases over time. If error correction is used, the usable gates are further restricted to a finite set.

Notable examples

There exists an uncountably infinite number of gates. Some of them have been named by various authors, and below follow some of those most often used in the literature.













Operator	Gate(s)	Matrix
Pauli-X (X)	 \oplus	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Fig.4: Examples of Quantum gates

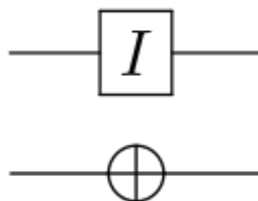
Identity gate:

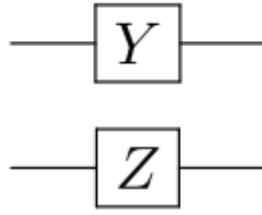
The identity gate is the identity matrix, usually written as I , and is defined for a single qubit as

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

where I is basis independent and does not modify the quantum state. The identity gate is most useful when describing mathematically the result of various gate operations or when discussing multi-qubit circuits.

Pauli gates (X,Y,Z) :





Quantum gates (from top to bottom): Identity gate, NOT gate, Pauli Y, Pauli Z

The Pauli gates (X, Y, Z) are the three Pauli matrices ($\sigma_x, \sigma_y, \sigma_z$) and act on a single qubit. The Pauli X, Y and Z equate, respectively, to a rotation around the x, y and z axes of the Bloch sphere by π radians.

The Pauli- X gate is the quantum equivalent of the NOT gate for classical computers with respect to the standard basis $|0\rangle, |1\rangle$, which distinguishes the z axis on the Bloch sphere. It is sometimes called a bit-flip as it maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. Similarly, the Pauli- Y maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$. Pauli Z leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. Due to this nature, Pauli Z is sometimes called phase-flip.

These matrices are usually represented as

$$\begin{aligned}
 X = \sigma_x = \text{NOT} &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\
 Y = \sigma_y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \\
 Z = \sigma_z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.
 \end{aligned}$$

The Pauli matrices are involutory, meaning that the square of a Pauli matrix is the identity matrix.

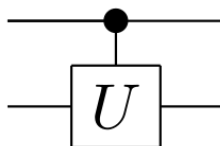
$$I^2 = X^2 = Y^2 = Z^2 = -iXYZ = I$$

The Pauli matrices also anti-commute, for example $ZX = iY = -XZ$.

The matrix exponential of a Pauli matrix σ_j is a rotation operator, often written as $e^{-i\sigma_j\theta/2}$.

Controlled gates:

Controlled gates act on 2 or more qubits, where one or more qubits act as a control for some operation. For example, the controlled NOT gate (or CNOT or CX) acts on 2 qubits, and performs the NOT operation on the second qubit only when the first qubit is $|1\rangle$, and otherwise leaves it unchanged. With respect to the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, it is represented by the Hermitian unitary matrix:



Circuit representation of
$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$
 controlled- U gate

The CNOT (or controlled Pauli- X) gate can be described as the gate that maps the basis states $|a, b\rangle \mapsto |a, a \oplus b\rangle$, where \oplus is XOR.

The CNOT can be expressed in the Pauli basis as:

$$\text{CNOT} = e^{i\frac{\pi}{4}(I-Z_1)(I-X_2)} = e^{-i\frac{\pi}{4}(I-Z_1)(I-X_2)}.$$

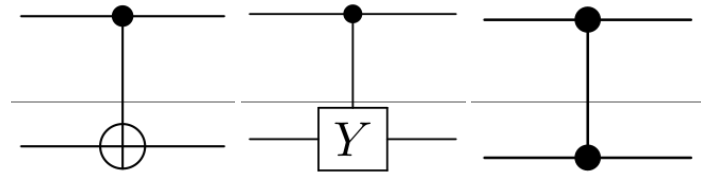
Being a Hermitian unitary operator, CNOT has the property $e^{i\theta U} = (\cos \theta)I + (i \sin \theta)U$ and $U = e^{i\frac{\pi}{2}(I-U)} = e^{-i\frac{\pi}{2}(I-U)}$, and is involutory.

More generally if U is a gate that operates on a single qubit with matrix representation

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix},$$

then the *controlled- U gate* is a gate that operates on two qubits in such a way that the first qubit serves as a control. It maps the basis states as follows.

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



Circuit diagrams of controlled Pauli gates (from left to right): CNOT (or controlled- X), controlled- Y and controlled- Z .

$$\begin{aligned} |10\rangle &\mapsto |1\rangle \otimes U|0\rangle = |1\rangle \otimes (u_{00}|0\rangle + u_{10}|1\rangle) \\ |11\rangle &\mapsto |1\rangle \otimes U|1\rangle = |1\rangle \otimes (u_{01}|0\rangle + u_{11}|1\rangle) \end{aligned}$$

The matrix representing the controlled U is

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}.$$

When U is one of the Pauli operators, X, Y, Z , the respective terms "controlled- X ", "controlled- Y ", or "controlled- Z " are sometimes used. Sometimes this is shortened to just CX, CY and CZ .

In general, any single qubit unitary gate can be expressed as $U = e^{iH}$, where H is a Hermitian matrix, and then the controlled U is $CU = e^{i\frac{1}{2}(I-Z_1)H_2}$.

Control can be extended to gates with arbitrary number of qubits and functions in programming languages. Functions can be conditioned on superposition states.

Phase shift gates:

The phase shift is a family of single-qubit gates that map the basis states $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\varphi}|1\rangle$. The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state. This is equivalent to tracing a horizontal circle (a line of constant latitude), or a rotation about the z-axis on the Bloch

sphere by φ radians. The phase shift gate is represented by the matrix:

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

where φ is the *phase shift* with the period 2π . Some common examples are the T gate where $\varphi = \frac{\pi}{4}$ (historically known as the $\pi/8$ gate), the phase gate (also known as the S gate, written as S , though S is sometimes used for SWAP gates) where $\varphi = \frac{\pi}{2}$ and

The phase shift gates are related to each other as follows:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P(\pi)$$

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = P\left(\frac{\pi}{2}\right) = \sqrt{Z}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} = P\left(\frac{\pi}{4}\right) = \sqrt{S} = \sqrt[4]{Z}$$

Note that the phase gate $P(\varphi)$ is not Hermitian (except for all

Hermitian conjugates: $P^\dagger(\varphi) = P(-\varphi)$

the PauliZ gate where $\varphi = \pi$. in instruction sets.^{[15][16]}

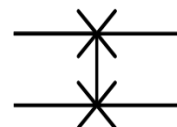
Swap gate:

The swap gate swaps two qubits. With respect to the basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, it is represented by the matrix

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

The swap gate can be decomposed into summation form:

$$\text{SWAP} = \frac{I \otimes I + X \otimes X + Y \otimes Y + Z \otimes Z}{2}$$



Circuit representation of swap gate

Hadamard gate:

The Hadamard or Walsh-Hadamard gate, named after Jacques Hadamard (French: [adamaʁ]) and Joseph L. Walsh, acts on a single qubit. It maps the basis

states $|0\rangle \mapsto \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle \mapsto \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ (it creates an equal superposition state if given a

computational basis state). The two states $(|0\rangle + |1\rangle)/\sqrt{2}$ and $(|0\rangle - |1\rangle)/\sqrt{2}$ are sometimes written $|+\rangle$ and $|-\rangle$ respectively. The Hadamard gate performs a rotation of π about the axis $(\hat{x} + \hat{z})/\sqrt{2}$ at the Bloch sphere, and is therefore involutory. It is represented by

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

the Hadamard matrix:



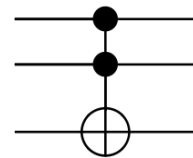
Circuit representation of Hadamard gate

If the Hermitian (so $H^\dagger = H^{-1} = H$) Hadamard gate is used to perform a change of basis, it flips \hat{x} and \hat{z} . For example, $HZH = X$ and $H\sqrt{X}H = \sqrt{Z} = S$.

Toffoli (CCNOT) gate

The Toffoli gate, named after Tommaso Toffoli and also called the CCNOT gate or Deutsch gate $D(\pi/2)$, is a 3-bit gate which is universal for classical computation but not for quantum computation. The quantum Toffoli gate is the same gate, defined for 3 qubits. If we limit ourselves to only accepting input qubits that are $|0\rangle$ and $|1\rangle$, then if the first two bits are in the state $|1\rangle$ it applies a Pauli-X (or NOT) on the third bit, else it does nothing. It is an example of a CC-U (controlled-controlled Unitary) gate. Since it is the quantum analog of a classical gate, it is completely specified by its truth table. The Toffoli gate is universal when combined with the single qubit Hadamard gate.^[17]

SWAP gate



Circuit representation of Toffoli gate

Truth table

INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Matrix form

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

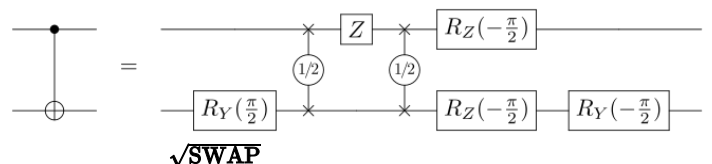
The Toffoli gate is related to the classical AND (\wedge) and XOR (\oplus) operations as it performs the mapping $|a, b, c\rangle \mapsto |a, b, c \oplus (a \wedge b)\rangle$ on states in the computational basis.

The Toffoli gate can be expressed using Pauli matrices as

$$\text{Toff} = e^{i\frac{\pi}{8}(I-Z_1)(I-Z_2)(I-X_3)} = e^{-i\frac{\pi}{8}(I-Z_1)(I-Z_2)(I-X_3)}.$$

Universal quantum gates

A set of universal quantum gates is any set of gates to which any operation possible on a quantum



computer can be reduced, that is, any other unitary operation can be expressed as a finite sequence of gates from the set.

Both CNOT and are universal two-qubit gates and can be uncountable set of gates since the number of possible transformed into each other. quantum gates is uncountable, whereas the number of finite sequences from a finite set is countable. To solve this problem, we only require that any quantum operation can be approximated by a sequence of gates from this finite set. Moreover, for unitaries on a constant number of qubits, the Solovay–Kitaev theorem guarantees that this can be done efficiently.

Some universal quantum gate sets include:

- The rotation operators $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$, the phase shift gate $P(\varphi)$ and CNOT are commonly used to form a universal quantum gate set.
- The Clifford set $\{\text{CNOT}, H, S\} + T$ gate. The Clifford set alone is not a universal quantum gate set, as it can be efficiently simulated classically according to the Gottesman–Knill theorem.

The Toffoli gate + Hadamard gate. The Toffoli gate alone forms a set of universal gates for reversible Boolean algebraic logic circuits which encompasses all classical computation.

Measurement :



Circuit representation of measurement. The two lines on the right hand side represent a classical bit, and the single line on the left hand side represents a qubit.

Measurement (sometimes called *observation*) is irreversible and therefore not a quantum gate, because it assigns the observed quantum state to a single value. Measurement takes a quantum state and projects it to one of the basis vectors, with a likelihood equal to the square of the vector's length along that basis vector. This is known as the Born rule and appears as a stochastic non-reversible operation as it probabilistically sets the quantum state equal to the basis vector that represents the measured state. At the instant of measurement, the state is said to "collapse" to the definite single value that was measured. Why and how, or even if the quantum state collapses at measurement, is called the measurement problem.

The probability of measuring a value with probability amplitude ϕ is $1 \geq |\phi|^2 \geq 0$, where $|\cdot|$ is the modulus.

Measuring a single qubit, whose quantum state is represented by the vector $a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$

. will result in $|0\rangle$ with probability $|a|^2$, and in $|1\rangle$ with probability $|b|^2$.

Quantum Algorithm

In quantum computing, a **quantum algorithm** is an algorithm which runs on a realistic model of quantum computation, the most commonly used model being the quantum circuit model of computation. A classical (or non-quantum) algorithm is a finite sequence of instructions, or a step-by-step procedure for solving a problem, where each step or instruction can be performed on a classical computer. Similarly, a quantum algorithm is a step-by-step procedure, where each of the steps can be performed on a quantum computer. Although all classical algorithms can also be performed on a quantum computer, the term quantum algorithm is usually used for those algorithms which seem inherently quantum, or use some essential feature of quantum computation such as quantum superposition or quantum entanglement.

Problems which are undecidable using classical computers remain undecidable using quantum computers. What makes quantum algorithms interesting is that they might be able to solve some problems faster than classical algorithms because the quantum superposition and quantum entanglement that quantum algorithms exploit probably cannot be efficiently simulated on classical computers (see Quantum supremacy).

The best-known algorithms are Shor's algorithm for factoring and Grover's algorithm for searching an unstructured database or an unordered list. Shor's algorithm runs much (almost exponentially) faster than the best-known classical algorithm for factoring, the general number field sieve. Grover's algorithm runs quadratically faster than the best possible classical algorithm for the same task, a linear search.

Overview

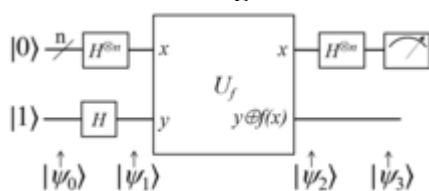
Quantum algorithms are usually described, in the commonly used circuit model of quantum computation, by a quantum circuit which acts on some input qubits and terminates with a measurement. A quantum circuit consists of simple quantum gates which act on at most a fixed number of qubits. The number of qubits has to be fixed because a changing number of qubits implies non-unitary evolution. Quantum algorithms may also be stated in other models of quantum computation, such as the Hamiltonian oracle model.

Quantum algorithms can be categorized by the main techniques used by the algorithm. Some commonly used techniques/ideas in quantum algorithms include phase kick-back, phase estimation, the quantum Fourier transform, quantum walks, amplitude amplification and topological quantum field theory. Quantum algorithms may also be grouped by the type of problem solved, for instance see the survey on quantum algorithms for algebraic problems.

Algorithms based on the quantum Fourier transform

The quantum Fourier transform is the quantum analogue of the discrete Fourier transform, and is used in several quantum algorithms. The Hadamard transform is also an example of a quantum Fourier transform over an n -dimensional vector space over the field \mathbb{F}_2 . The quantum Fourier transform can be efficiently implemented on a quantum computer using only a polynomial number of quantum gates.

Deutsch–Jozsa algorithm



Deutsch-Jozsa algorithm

The Deutsch–Jozsa algorithm solves a black-box problem which probably requires exponentially many queries to the black box for any deterministic classical computer, but can be done with one query by a quantum computer. However, when comparing bounded-error classical and quantum algorithms, there is no speedup since a classical probabilistic algorithm can solve the problem with a constant number of queries with small probability of error. The algorithm determines whether a function f is either constant (0 on all inputs or 1 on all inputs) or balanced (returns 1 for half of the input domain and 0 for the other half).

Bernstein–Vazirani algorithm

The Bernstein–Vazirani algorithm is the first quantum algorithm that solves a problem more efficiently than the best known classical algorithm. It was designed to create an oracle separation between BQP and BPP.

Simon's algorithm

Simon's algorithm solves a black-box problem exponentially faster than any classical algorithm, including bounded-error probabilistic algorithms. This algorithm, which achieves an exponential speedup over all classical algorithms that we consider efficient, was the motivation for Shor's factoring algorithm.

Quantum phase estimation algorithm

The quantum phase estimation algorithm is used to determine the eigenphase of an eigenvector of a unitary gate given a quantum state proportional to the eigenvector and access to the gate. The algorithm is frequently used as a subroutine in other algorithms.

Shor's algorithm

Shor's algorithm solves the discrete logarithm problem and the integer factorization problem in polynomial time, whereas the best known classical algorithms take super-polynomial time. These problems are not known to be in P or NP-complete. It is also one of the few quantum algorithms that solves a non-black-box problem in polynomial time where the best known classical algorithms run in super-polynomial time.

Hidden subgroup problem

The abelian hidden subgroup problem is a generalization of many problems that can be solved by a quantum computer, such as Simon's problem, solving Pell's equation, testing the principal ideal of a ring R and factoring. There are efficient quantum algorithms known for the Abelian hidden subgroup problem. The more general hidden subgroup problem, where the group isn't necessarily abelian, is a generalization of the previously mentioned problems and graph isomorphism and certain lattice problems. Efficient quantum algorithms are known for certain non-abelian groups. However, no efficient algorithms are known for the symmetric group, which would give an efficient algorithm for graph isomorphism and the dihedral group, which would solve certain lattice problems.

Estimating Gauss sums

A Gauss sum is a type of exponential sum. The best known classical algorithm for estimating these sums takes exponential time. Since the discrete logarithm problem reduces to Gauss sum estimation, an efficient classical algorithm for estimating Gauss sums would imply an efficient classical algorithm for computing discrete logarithms, which is considered unlikely. However, quantum computers can estimate Gauss sums to polynomial precision in polynomial time.

Fourier fishing and Fourier checking

We have an oracle consisting of n random Boolean functions mapping n -bit strings to a Boolean value. We are required to find n n -bit strings z_1, \dots, z_n such that for the Hadamard-Fourier transform, at least $3/4$ of the strings satisfy

$$|\tilde{f}(z_i)| \geq 1$$

and at least $1/4$ satisfies

$$|\tilde{f}(z_i)| \geq 2.$$

This can be done in bounded-error quantum polynomial time (BQP).

Algorithms based on amplitude amplification

Amplitude amplification is a technique that allows the amplification of a chosen subspace of a quantum state. Applications of amplitude amplification usually lead to quadratic speedups over the corresponding classical algorithms. It can be considered to be a generalization of Grover's algorithm.

Grover's algorithm

Grover's algorithm searches an unstructured database (or an unordered list) with N entries, for a marked entry, using only $O(\sqrt{N})$ queries instead of the $O(N)$ queries required classically. Classically, $O(N)$ queries are required even allowing bounded-error probabilistic algorithms.

Theorists have considered a hypothetical generalization of a standard quantum computer that could access the histories of the hidden variables in Bohmian mechanics. (Such a computer is completely hypothetical and would *not* be a standard quantum computer, or even possible under the standard theory of quantum mechanics.) Such a hypothetical computer could implement a search of an N -item database at most in $O(\sqrt[3]{N})$ steps. This is slightly faster than the $O(\sqrt{N})$ steps taken by Grover's algorithm. Neither search method would allow either model of quantum computer to solve NP-complete problems in polynomial time.

Quantum counting

Quantum counting solves a generalization of the search problem. It solves the problem of counting the number of marked entries in an unordered list, instead of just detecting if one exists.

Specifically, it counts the number of marked entries in an N -element list, with error ϵ making only

$\Theta\left(\frac{1}{\epsilon} \sqrt{\frac{N}{k}}\right)$ queries, where k is the number of marked elements in the list.^{[17][18]} More precisely,

the algorithm outputs an estimate k' , the number of marked entries, with the following accuracy:

$$|k - k'| \leq \epsilon k$$

Algorithms based on quantum walks

A quantum walk is the quantum analogue of a classical random walk, which can be described by a probability distribution over some states. A quantum walk can be described by a quantum superposition over states. Quantum walks are known to give exponential speedups for some

black-box problems. They also provide polynomial speedups for many problems. A framework for the creation of quantum walk algorithms exists and is quite a versatile tool.

Boson sampling problem

The Boson Sampling Problem in an experimental configuration assumes an input of bosons (ex. photons of light) of moderate number getting randomly scattered into a large number of output modes constrained by a defined unitarity. When individual photons of light are used the problem is isomorphic to a multi-photon quantum walk. The problem is then to produce a fair sample of the probability distribution of the output which is dependent on the input arrangement of bosons and the Unitarity. Solving this problem with a classical computer algorithm requires computing the permanent of the unitary transform matrix, which may be either impossible or take a prohibitively long time. In 2014, it was proposed that existing technology and standard probabilistic methods of generating single photon states could be used as input into a suitable quantum computable linear optical network and that sampling of the output probability distribution would be demonstrably superior using quantum algorithms. In 2015, investigation predicted the sampling problem had similar complexity for inputs other than Fock state photons and identified a transition in computational complexity from classically simulatable to just as hard as the Boson Sampling Problem, dependent on the size of coherent amplitude inputs

Element distinctness problem

The element distinctness problem is the problem of determining whether all the elements of a list are distinct. Classically, $\Omega(N)$ queries are required for a list of size N . However, it can be solved in $\Theta(N^{2/3})$ queries on a quantum computer. The optimal algorithm is by Andris Ambainis. Yaoyun Shi first proved a tight lower bound when the size of the range is sufficiently large. Ambainis and Kutin independently (and via different proofs) extended his work to obtain the lower bound for all functions.

Triangle-finding problem

The triangle-finding problem is the problem of determining whether a given graph contains a triangle (a clique of size 3). The best-known lower bound for quantum algorithms is $\Omega(N)$, but the best algorithm known requires $O(N^{1.297})$ queries, an improvement over the previous best $O(N^{1.3})$ queries.

Formula evaluation

A formula is a tree with a gate at each internal node and an input bit at each leaf node. The problem is to evaluate the formula, which is the output of the root node, given oracle access to the input.

A well studied formula is the balanced binary tree with only NAND gates. This type of formula requires $\Theta(N^c)$ queries using randomness, where $c = \log_2(1 + \sqrt{33})/4 \approx 0.754$. With a quantum algorithm however, it can be solved in $\Theta(N^{0.5})$ queries. No better quantum algorithm

for this case was known until one was found for the unconventional Hamiltonian oracle model. The same result for the standard setting soon followed.

Fast quantum algorithms for more complicated formulas are also known.

Quantum simulation

The idea that quantum computers might be more powerful than classical computers originated in Richard Feynman's observation that classical computers seem to require exponential time to simulate many-particle quantum systems. Since then, the idea that quantum computers can simulate quantum physical processes exponentially faster than classical computers has been greatly fleshed out and elaborated. Efficient (that is, polynomial-time) quantum algorithms have been developed for simulating both Bosonic and Fermionic systems and in particular, the simulation of chemical reactions beyond the capabilities of current classical supercomputers requires only a few hundred qubits. Quantum computers can also efficiently simulate topological quantum field theories. In addition to its intrinsic interest, this result has led to efficient quantum algorithms for estimating quantum topological invariants such as Jones and HOMFLY polynomials, and the Turaev-Viro invariant of three-dimensional manifolds.

Solving a linear systems of equations

In 2009 Aram Harrow, Avinatan Hassidim, and Seth Lloyd, formulated a quantum algorithm for solving linear systems. The algorithm estimates the result of a scalar measurement on the solution vector to a given linear system of equations.

Provided the linear system is a sparse and has a low condition number κ , and that the user is interested in the result of a scalar measurement on the solution vector, instead of the values of the solution vector itself, then the algorithm has a runtime of $O(\log(N)\kappa^2)$, where N is the number of variables in the linear system. This offers an exponential speedup over the fastest classical algorithm, which runs in $O(N\kappa)$ (or $O(N\sqrt{\kappa})$ for positive semidefinite matrices).

Hybrid quantum/classical algorithms

Hybrid Quantum/Classical Algorithms combine quantum state preparation and measurement with classical optimization. These algorithms generally aim to determine the ground state eigenvector and eigenvalue of a Hermitian Operator.

QAOA

The quantum approximate optimization algorithm is a toy model of quantum annealing which can be used to solve problems in graph theory. The algorithm makes use of classical optimization of quantum operations to maximize an objective function.

Variational quantum eigensolver

The variational quantum eigensolver (VQE) algorithm applies classical optimization to minimize the energy expectation of an ansatz state to find the ground state energy of a molecule. This can also be extended to find excited energies of molecules.

Contracted quantum eigensolver

The CQE algorithm minimizes the residual of a contraction (or projection) of the Schrödinger equation onto the space of two (or more) electrons to find the ground- or excited-state energy and two-electron reduced density matrix of a molecule. It is based on classical methods for

solving energies and two-electron reduced density matrices directly from the anti-Hermitian contracted Schrödinger equation.

Quantum Error Correction

Quantum error correction (QEC) is used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise. Quantum error correction is theorised as essential to achieve fault tolerant quantum computing that can reduce the effects of noise on stored quantum information, faulty quantum gates, faulty quantum preparation, and faulty measurements. This would allow algorithms of greater circuit depth.

Classical error correction employs redundancy. The simplest albeit inefficient approach is the repetition code. The idea is to store the information multiple times, and—if these copies are later found to disagree—take a majority vote; e.g. suppose we copy a bit in the one state three times. Suppose further that a noisy error corrupts the three-bit state so that one of the copied bits is equal to zero but the other two are equal to one. Assuming that noisy errors are independent and occur with some sufficiently low probability p , it is most likely that the error is a single-bit error and the transmitted message is three ones. It is possible that a double-bit error occurs and the transmitted message is equal to three zeros, but this outcome is less likely than the above outcome. In this example, the logical information was a single bit in the one state, the physical information are the three copied bits, and determining what logical state is encoded in the physical state is called *decoding*. Similar to classical error correction, QEC codes do not always correctly decode logical qubits, but their use reduces the effect of noise.

Copying quantum information is not possible due to the no-cloning theorem. This theorem seems to present an obstacle to formulating a theory of quantum error correction. But it is possible to *spread* the (logical) information of one qubit onto a highly entangled state of several (physical) qubits. Peter Shor first discovered this method of formulating a *quantum error correcting code* by storing the information of one qubit onto a highly entangled state of nine qubits.

Classical error correcting codes use a *syndrome measurement* to diagnose which error corrupts an encoded state. An error can then be reversed by applying a corrective operation based on the syndrome. Quantum error correction also employs syndrome measurements. It performs a multi-qubit measurement that does not disturb the quantum information in the encoded state but retrieves information about the error. Depending on the QEC code used, syndrome measurement can determine the occurrence, location and type of errors. In most QEC codes, the type of error is either a bit flip, or a sign (of the phase) flip, or both (corresponding to the Pauli matrices X, Z, and Y). The measurement of the syndrome has the projective effect of a quantum measurement, so even if the error due to the noise was arbitrary, it can be expressed as a combination of basis operations called the error basis (which is given by the Pauli matrices and the identity). To correct the error, the Pauli operator corresponding to the type of error is used on the corrupted qubit to revert the effect of the error.

The syndrome measurement provides information about the error that has happened, but not about the information that is stored in the logical qubit—as otherwise the measurement would destroy any quantum superposition of this logical qubit with other qubits in the quantum computer, which would prevent it from being used to convey quantum information.

Models

Over time, researchers have come up with several codes:

- Peter Shor's 9-qubit-code, a.k.a. the Shor code, encodes 1 logical qubit in 9 physical qubits and can correct for arbitrary errors in a single qubit.
- Andrew Steane found a code that does the same with 7 instead of 9 qubits, see Steane code.
- Raymond Laflamme and collaborators found a class of 5-qubit codes that do the same, which also have the property of being fault-tolerant. A 5-qubit code is the smallest possible code that protects a single logical qubit against single-qubit errors.
- A generalisation of the technique used by Steane, to develop the 7-qubit code from the classical [7, 4] Hamming code, led to the construction of an important class of codes called the CSS codes, named for their inventors: Robert Calderbank, Peter Shor and Andrew Steane. According to the quantum Hamming bound, encoding a single logical qubit and providing for arbitrary error correction in a single qubit requires a minimum of 5 physical qubits.
- A more general class of codes (encompassing the former) are the stabilizer codes discovered by Daniel Gottesman, and by Robert Calderbank, Eric Rains, Peter Shor, and N. J. A. Sloane; these are also called additive codes.
- Two dimensional Bacon–Shor codes are a family of codes parameterized by integers m and n . There are nm qubits arranged in a square lattice.
- A newer idea is Alexei Kitaev's topological quantum codes and the more general idea of a topological quantum computer.
- Todd Brun, Igor Devetak, and Min-Hsiu Hsieh also constructed the entanglement-assisted stabilizer formalism as an extension of the standard stabilizer formalism that incorporates quantum entanglement shared between a sender and a receiver.

That these codes allow indeed for quantum computations of arbitrary length is the content of the quantum threshold theorem, found by Michael Ben-Or and Dorit Aharonov, which asserts that you can correct for all errors if you concatenate quantum codes such as the CSS codes—i.e. re-encode each logical qubit by the same code again, and so on, on logarithmically many levels—*provided* that the error rate of individual quantum gates is below a certain threshold; as otherwise, the attempts to measure the syndrome and correct the errors would introduce more new errors than they correct for.

As of late 2004, estimates for this threshold indicate that it could be as high as 1–3%, provided that there are sufficiently many qubits available.

Experimental realization

There have been several experimental realizations of CSS-based codes. The first demonstration was with nuclear magnetic resonance qubits. Subsequently, demonstrations have been made with linear optics, trapped ions, and superconducting (transmon) qubits.

In 2016 for the first time the lifetime of a quantum bit was prolonged by employing a QEC code. The error-correction demonstration was performed on Schrodinger-cat states encoded in a superconducting resonator, and employed a quantum controller capable of performing real-time feedback operations including read-out of the quantum information, its analysis, and the correction of its detected errors. The work demonstrated how the quantum-error-corrected

system reaches the break-even point at which the lifetime of a logical qubit exceeds the lifetime of the underlying constituents of the system (the physical qubits).

Other error correcting codes have also been implemented, such as one aimed at correcting for photon loss, the dominant error source in photonic qubit schemes.

In 2021, an entangling gate between two logical qubits encoded in topological quantum error-correction codes has first been realized using 10 ions in a trapped-ion quantum computer. 2021 also saw the first experimental demonstration of fault-tolerant Bacon-Shor code in a single logical qubit of a trapped-ion system, i.e. a demonstration for which the addition of error correction is able to suppress more errors than is introduced by the overhead required to implement the error correction as well as fault tolerant Steane code.

In 2022, researchers at the University of Innsbruck have demonstrated a fault-tolerant universal set of gates on two logical qubits in a trapped-ion quantum computer. They have performed a logical two-qubit controlled-NOT gate between two instances of the seven-qubit colour code, and fault-tolerantly prepared a logical magic state.

In February 2023 researchers at Google claimed to have decreased quantum errors by increasing the qubit number in experiments, they used a fault tolerant surface code measuring an error rate of 3.028% and 2.914% for a distance-3 qubit array and a distance-5 qubit array respectively.

Current Challenges

Despite the incredible potential of quantum computing, there are still significant challenges that need to be addressed before this technology can become a reliable and practical tool. One of the most prominent challenges is the issue of noise and stability in quantum systems. In this section, we will explore the factors contributing to noise, the impact of this challenge on quantum computing, and the ongoing efforts to overcome it – all while maintaining a tone that is engaging for both search engines and users.

Quantum computers rely on delicate quantum states that are highly susceptible to disturbances from their surrounding environment. Factors such as temperature, electromagnetic radiation, and even cosmic rays can introduce errors into a quantum system, leading to computational inaccuracies. This sensitivity to external influences is known as quantum noise.

Noise is particularly problematic for quantum computing due to the fragile nature of qubits, which can quickly lose their quantum properties – a process called decoherence. Decoherence leads to a loss of the very features that make quantum computing so powerful, such as superposition and entanglement. As a result, mitigating noise and increasing qubit stability are critical for building practical and reliable quantum computers.

1. ERROR CORRECTION

Most experts would consider this the biggest challenge. Quantum computers are extremely sensitive to noise and errors caused by interactions with their environment. This can cause errors to accumulate and degrade the quality of computation. Developing reliable error correction techniques is therefore essential for building practical quantum computers.

2. SCALABILITY

While quantum computers have shown impressive performance for some tasks, they are still relatively small compared to classical computers. Scaling up quantum computers to hundreds or thousands of qubits while maintaining high levels of coherence and low error rates remains a major challenge.

3. HARDWARE DEVELOPMENT

Developing high-quality quantum hardware, such as qubits and control electronics, is a major challenge. There are many different qubit technologies, each with its own strengths and weaknesses, and developing a scalable, fault-tolerant qubit technology is a major focus of research.

1. **Qubit Design:** Advances in qubit design and materials can lead to more stable and noise-resistant qubits. For example, researchers are exploring topological qubits, which leverage the unique properties of certain materials to protect quantum information from noise-induced errors.

4. SOFTWARE DEVELOPMENT

Quantum algorithms and software development tools are still in their infancy, and there is a need for new programming languages, compilers, and optimization tools that can effectively utilize the power of quantum computers.

5. CLASSICAL COMPUTERS INTERFACES

Quantum computers won't replace classical computers; they will serve as complementary technology. Developing efficient and reliable methods for transferring data between classical and quantum computers is essential for practical applications.

1. **Cooling and Isolation:** Reducing the temperature and isolating quantum systems from their environment can help minimize noise and enhance stability. Some quantum computers, such as those based on superconducting qubits, operate at extremely low temperatures to achieve this goal.

6. STANDARDS AND PROTOCOLS

As the field of quantum computing matures, there is a need for standards and protocols for hardware, software, and communication interfaces. Developing these standards will be essential for ensuring compatibility and interoperability between different quantum computing platforms. We should also throw in benchmarking — the ability to measure performance standards is still in its infancy for quantum computing design, development and operation.

7. TRAINED TALENT

The number of people properly educated and trained to enter the quantum workforce is small and spread across the world. Finding the right workers is a challenge. In a chicken-and-egg scenario, we won't increase the number of people motivated to enter the quantum workforce until we have more practical quantum computers and we won't have more practical quantum computers until we have more people motivated to become part of the quantum workforce.

8. OVERALL EXPENSE

Perhaps this is an obvious outcome of all the above challenges, but expense remains a huge roadblock — or stumbling block — for quantum computing. The likelihood that two Steves will be slapping together quantum computers in their garage is an unlikely scenario. Quantum talent is expensive. Quantum hardware is expensive. Supply chains are complex, vulnerable and — you guessed it — expensive to establish and maintain. Dealing with these expenses and finding investments to offset these costs will likely be a standard duty of institutional scientists and commercial entrepreneurs for the foreseeable future.

Future prospects

Quantum computing's unique capabilities have the potential to revolutionize problem-solving across various domains. By harnessing the power of qubits and the principles of quantum mechanics, quantum computers can tackle problems that have long remained unsolvable or required excessive time and resources using classical computers. In this section.

1. **Optimization Problems:** Quantum computing has the potential to transform how we approach optimization problems, which involve finding the best solution among a vast number of possibilities. Examples include supply chain optimization, traffic routing, and portfolio management. By exploiting quantum parallelism, these computers can evaluate multiple solutions at once, dramatically reducing the time required to find the optimal solution.
2. **Cryptography:** One of the most prominent applications of quantum computing lies in the realm of cryptography. Quantum computers can potentially crack existing encryption methods, such as RSA and elliptic curve cryptography, which are currently considered secure. However, this also presents an opportunity for developing new, quantum-resistant cryptographic algorithms, ensuring data security in a post-quantum world.
3. **Drug Discovery:** Quantum computing can revolutionize drug discovery by simulating molecular interactions at the quantum level. This capability allows researchers to predict how a drug candidate will interact with its target, potentially speeding up the drug development process and reducing costs.
4. **Artificial Intelligence and Machine Learning:** Quantum computing can enhance machine learning algorithms by performing complex calculations and pattern recognition at a much faster rate than classical computers. This acceleration can lead to significant advancements in AI, including improved natural language processing, image recognition, and predictive analytics.
5. **Climate Modelling:** Quantum computers can simulate complex systems, such as climate models, with much greater accuracy than classical computers. This improved modelling can lead to better predictions of climate change impacts and help inform policy decisions.

Quantum computing also has potential applications across various industries like

1. **Finance:** Quantum computing has the potential to revolutionize financial services by optimizing trading strategies, portfolio management, and risk assessment. By handling complex calculations at unprecedented speeds, quantum computers can enable more accurate predictions of market trends and enhance decision-making processes in finance.

2. **Healthcare:** The healthcare industry stands to benefit immensely from quantum computing. By simulating molecular interactions and biological processes, quantum computers can accelerate drug discovery, improve personalized medicine, and optimize treatment plans. Additionally, these computers can assist in analyzing large-scale genomic data, leading to breakthroughs in understanding the genetic basis of diseases.
3. **Energy:** Quantum computing can transform the energy sector by optimizing energy distribution, improving grid management, and enhancing renewable energy storage. It can also aid in the discovery of new materials for more efficient solar cells and batteries, contributing to a more sustainable future.
4. **Telecommunications:** Quantum computing can enhance network optimization and traffic routing in telecommunications, ensuring more efficient use of resources and reducing latency. Moreover, it has the potential to enable ultra-secure communication through quantum cryptography, safeguarding sensitive data transmission.
5. **Supply Chain and Logistics:** Quantum computers can optimize complex supply chain networks, allowing companies to minimize costs, reduce waste, and improve delivery times. By analyzing vast amounts of data and considering numerous variables simultaneously, quantum computing can streamline logistics operations and enhance overall efficiency.
6. **Aerospace and Defense:** Quantum computing can aid in the design and simulation of advanced materials and complex systems, leading to more efficient aircraft and space vehicles. It also has the potential to improve satellite-based navigation systems and enhance the security of military communications.

The power of quantum computing offers unprecedented problem-solving capabilities across various fields, from optimization problems to drug discovery. As this technology continues to develop, it will undoubtedly unlock new possibilities and reshape our approach to solving complex challenges.

Conclusion

Quantum computing stands on the brink of a transformative era in computing and information processing. By leveraging the peculiar laws of quantum physics, quantum computing has the potential to tackle problems that are practically intractable for classical computers. As research continues and technologies mature, quantum computing is poised to revolutionize industries and drive innovation in ways we have yet to fully comprehend.

References:

1. **Quantum Mechanics Basics:** https://en.wikipedia.org/wiki/Introduction_to_quantum_mechanics
2. **The Birth of Quantum Computing:** https://en.wikipedia.org/wiki/Quantum_computing
3. **Quantum Bits (Qubits):** <https://en.wikipedia.org/wiki/Qubit>
4. **Quantum Gates and Circuits:** https://en.wikipedia.org/wiki/Quantum_logic_gate#Notable_examples
5. **Quantum Algorithms:** https://en.wikipedia.org/wiki/Quantum_algorithm
6. **Quantum Error Correction:** https://en.wikipedia.org/wiki/Quantum_error_correction
7. **Current Challenges and Future Prospects:** <https://vegibit.com/the-future-of-quantum-computing-challenges-and-opportunities/>