How to Build a Quantum Computer

Barry Sanders explains why physicists want to build a quantum computer, how it could work and when it will be ready.

physicsworld Discovery

How to Build a Quantum Computer

How to Build a Quantum Computer

Barry C Sanders
University of Calgary, Canada and University of Science and Technology of China

IOP Publishing, Bristol, UK

ISBN 978-0-7503-1536-4 (ebook)

DOI 10.1088/978-0-7503-1536-4

Version: 20171101

Physics World Discovery
ISSN 2399-2891 (online)

British Library Cataloguing-in-Publication Data: A catalogue record for this book is available from the British Library.

Published by IOP Publishing, wholly owned by The Institute of Physics, London

IOP Publishing, Temple Circus, Temple Way, Bristol, BS1 6HG, UK

US Office: IOP Publishing, Inc., 190 North Independence Mall West, Suite 601, Philadelphia, PA 19106, USA

To the elusive eternal universal truth.

Contents

Abstract

Quantum computer technology is progressing rapidly with dozens of qubits and hundreds of quantum logic gates now possible. Although current quantum computer technology is distant from being able to solve computational problems beyond the reach of non-quantum computers, experiments have progressed well beyond simply demonstrating the requisite components. We can now operate small quantum logic processors with connected networks of qubits and quantum logic gates, which is a great stride towards functioning quantum computers. This book aims to be accessible to a broad audience with basic knowledge of computers, electronics and physics. The goal is to convey key notions relevant to building quantum computers and to present state-of-the-art quantum-computer research in various media such as trapped ions, superconducting circuits, photonics and beyond.

Acknowledgments

I am grateful to the Canadian Institute for Advanced Research for including me in the Quantum Information Science Program through which I learned deeply the interdisciplinary aspects of quantum information, including physics, computer science, mathematics and engineering. I also appreciate *i*CORE, which later morphed into Alberta Innovates through some intermediate incarnations, for believing enough in quantum computing, and in me as a quantum computing researcher, to support me as a research chair professor from 2003 to 2017. Of course, I owe an infinite debt of gratitude to many. I especially want to thank my mentors, colleagues, collaborators, mentees, and above all my loving families: both my family of origin and my family of procreation.

Author biography

Barry C Sanders

Barry C Sanders is the director of the Institute for Quantum Science and Technology at the University of Calgary, Canada and holds a Thousand Talents Chair in the National Laboratory for Physical Sciences at the Microscale at the University of Science and Technology China. His BSc degree is from the University of Calgary and he completed a Diploma of Imperial College London supervised by Sir Thomas Kibble followed by a PhD at Imperial College London supervised by Sir Peter Knight. He was a postdoctoral fellow at the Australian National University and the Universities of Queensland and Waikato and then was a Macquarie University professor from 1991 to 2003. In 2003, Sanders joined the University of Calgary as an *i*CORE chair and later Alberta Innovates–Technology Futures chair.

Sanders is especially well known for seminal contributions to theories of quantum-limited measurement, highly non-classical light, practical quantum cryptography and optical implementations of quantum information tasks. His current research interests include quantum resources and algorithms; optical and atomic implementations of quantum information tasks and protocols; quantum processes in biological systems; and machine learning for quantum control. He is a fellow of the Royal Society of Canada, the Institute of Physics (UK), the Optical Society of America and the American Physical Society. Sanders is also a senior fellow of the Canadian Institute for Advanced Research. In 2016 Sanders was awarded a DSc by Imperial College London.

Sanders's leadership roles include being a former president of the Australian Optical Society; founding co-chair of the Canadian Association of Physicists Division of Atomic, Molecular and Optical Physics; and founding leader of the Optical Society of America Quantum Optical Science and Technology Technical Group. He is editor-in-chief of *New Journal of Physics*; a former remote-staff associate editor of *Physical Review A*; a former editor of *Optics Communications*; and a former editor of *Mathematical Structures of Computer Science*.

How to Build a Quantum Computer

Barry C Sanders

1 Introduction

What is a quantum computer and why do we want to build one?

Without a doubt, we live in a digital age. Communication has transitioned from analogue information, such as sound waves or electrical pulses, to digital streams of zeroes and ones (bit strings). Digital computation has revolutionized our lives, providing vast knowledge at our fingertips, computer-aided design, rapid solutions to vital mathematical problems, quantitative finance and prognosticating climate change.

The digital world is astonishing in so many ways, but what if the digital world weren't the whole story? What if something more powerful lurked below the surface, something that contained all our digital communication and computation as a special case, something that generalized our digital capability and showed promise of even greater capability?

Something more powerful does lurk beneath: quantum information contains our current notion of digital information as a special case and it exceeds the capability provided by processing digital information alone. Since 1900, scientists have known that all of nature is underpinned by the seemingly strange rules of quantum mechanics: matter and energy manifests as tiny indivisible particles or else as extended interfering waves depending on how the measurement is performed. Particles and waves are contradictory notions, yet both descriptions are tied together neatly in the mathematics of quantum mechanics. Quantum scientists refer to pre-quantum notions of the world as *classical*.

Philosophically, quantum mechanics has an inherent puzzle known as the measurement paradox. Despite this paradox, quantum mechanics properly describes the Universe as we see it. Beginning in 1970 with Stephen Wiesner's notion of quantum money, and followed by the realization that quantum information cannot be copied, the first foundations of quantum information were established. These notions were soon followed by potential applications: quantum communication that is secure against any computational attack and quantum computing that solves some computational problems faster than can be achieved by classical algorithms.

doi:10.1088/978-0-7503-1536-4ch1

Quantum information could offer great benefits, but let us focus on building a quantum computer—what is required, what has been done, and what is left to do. To this end, we think of the quantum computer simply as a (classical) computer that accepts a bit-string input and yields a bit-string output. However, this computer is augmented with a quantum processor that executes any quantum algorithm. A quantum algorithm has classical input and output bit strings but has operations constructed with quantum-logic gates. The computer reuses the quantum processor as often as needed and then processes all the classical outputs to solve the computational problem.

To understand the quantum processor, we must first understand an important fact about classical computing: that a circuit designed to solve a decision problem (answer is yes = 1 or no = 0) can be expressed as a Boolean function, which maps bit strings to one bit. Remarkably, this Boolean function can be decomposed into a sequence of one- and two-bit gates, such as the NOT gate (flips 0 to 1 and vice versa) and XOR gate (adds two bits modulus 2). This decomposition makes constructing scalable hardware relatively simple. To make a universal circuit of any size we must build gates well enough; devise sufficiently good interconnects between gates; and add error correction to compensate for imperfections.

Building a quantum computer relies on the same principle. We need to build a universal set of gates such that any quantum program—technically a 'unitary transformation' that maps a quantum state to a quantum state—can be expressed efficiently and with high accuracy by a circuit comprising such gates. These gates and their requirements are described in the next section.

2 Background

Quantum information and algorithms

Quantum information is represented as qubit ('quantum bit') strings that are types of quantum states. One qubit can be prepared in either logic state $|0\rangle$ or $|1\rangle$, with bit values 0 and 1 encased in what is called a 'ket', which denotes a quantum state. Classically, a bit is either 0 or 1, but, quantumly, the state can be in a superposition of $|0\rangle$ or $|1\rangle$, meaning that the qubit could be observed as 0 or 1 in a random, probabilistic sense and, moreover, can interfere with other qubits such that qubits behave in a wavelike fashion.

Two qubits can be prepared in a superposition of $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$, which can be an entangled quantum informational state. The numbers 00, 01, 10 and 11 are binary representations of the base-10 numbers 0, 1, 2 and 3 so the state could be expressed in base-10 as $|0\rangle+|1\rangle+|2\rangle+|3\rangle$, meaning a superposition of all numbers from zero to three. Extending this notion, an entangled state of many qubits could be an equal superposition of all possible numbers representable by that finite bit string. A good quantum algorithm exploits wavelike interference during processing of such superpositions of numbers to solve efficiently some computational problems that would be intractable otherwise.

Physically, the qubit is manifested as a two-level system. For example, the up spin of an electron or a nucleus could be $|0\rangle$ and the down spin $|1\rangle$. Similarly, the

polarization of a single photon can be $|0\rangle$ or $|1\rangle$. A single atom whose outermost electron is energetically excited can be expressed as being in the state $|1\rangle$ and the lowest-energy, or 'ground', state is $|0\rangle$.

In 1994, Peter Shor presented two remarkable results: one showing that a quantum computer would provide exponential speedup for number factorization and the other showing that quantum error correction could circumvent decoherence. Decoherence is the inevitable deterioration of a quantum state over time and had hitherto been regarded as destroying any advantage quantum computing could offer. Suddenly the scientific community was abuzz with generating ideas for making a quantum computer. Quantum computing proposals included using nuclear spin or electron spin or electron energy within an atom or photon path or polarization.

The first strong reason to build a quantum computer is provided by Shor's other monumental contribution: a quantum algorithm that is faster than all *known* classical factorization algorithms and *believed* to be faster than all classical algorithms. In contrast, Grover's quantum search algorithm is *provably* faster than a classical search of an unsorted database, but it is only quadratically faster. In addition to the fundamental importance of a provably faster quantum algorithm, Grover's algorithm has potential significant applications. Other historical algorithms include the Deutsch–Jozsa and Bernstein–Vazirani quantum algorithms. More recently, quantum simulation, linear equation and optimization have joined the suite of quantum algorithms, but not always exhibiting a proven quantum speedup yet arguably having important practical applications.

The two-qubit Deutsch–Jozsa algorithm is often the first computation demonstrated on a newly minted two-qubit quantum computer. This algorithm solves whether an unknown Boolean function is either constant (always yields either 0 or 1 for every input) or balanced (answers are 0 in half the cases and 1 in the other half of cases) when such a function is promised to be either constant or balanced and nothing else.

Loosely speaking, the speed of an algorithm is quantified by the length of the shortest computational circuit executing the algorithm, hence roughly how long it takes to run. The complexity of the circuit relates how this length scales with the number of bits required to specify the input. For example, an exponentially faster algorithm has a run time that is exponentially smaller than how much time the best known classical algorithm takes to solve the same problem. A quadratically faster algorithm means that the quantum algorithm run-time scales as the square root of the run time for the classical algorithm to solve the same problem.

With respect to hardware development, qubits need to be individually addressable. Placing physical qubits into a regular lattice structure of one, two or three physical dimensions is an appealing architecture. Atoms could be charged, as ions, and electrically trapped in a lattice structure, or neutral atoms could be held in a lattice structure via intersecting laser beams holding atoms in place by light-atom forces. Alternatively, solid realizations of artificial atoms using superconductors or semiconductors are also enticing. In a completely different vein, photons could serve as viable qubits. One realization is as flying packets of energy interacting via

material media, or else trapped temporarily in regions with reflecting surfaces such as mirrors.

DiVincenzo's criteria

Many possible qubits and gates can be imagined, so in 2000 David DiVincenzo wrote five criteria to assess various proposals, which I remember by the abbreviation MUSIC.

- **M**easurable: the quantum output string can be read qubit-by-qubit.
- **U**niversal: a feasible universal set of quantum logic gates so arbitrary quantum algorithms can be expressed as a sequence of these gates.
- **S**calable: the computer can be enlarged to more qubits and quantum logical gates with low enough cost that the quantum advantage is not removed.
- **I**nitializable: the qubit string can be prepared all in the ($|0\rangle$) state.
- **C**oherent: quantum logic operations are sufficiently impervious to decoherence so quantum error correction strategies work with scalable overhead.

Fault tolerance is a crucial requirement behind these principles. Provided that good qubits and gates can be made, imperfect preparation, encoding, processing, decoding and readout can be ameliorated efficiently.

Following from these criteria, measures of success focus on components such as determining the quality of a qubit or the performance of a quantum logic gate. 'Fidelity' is a typical figure of merit, which quantifies how much the actual and desired results 'overlap'. On the other hand, scalability of quantum computing depends on error rates and the use of quantum error correction to reduce these errors rates. Another approach to assessing progress in experimental quantum computing is just to prepare nonclassical states, such as entangled states. Alternatively, one executes a quantum task such as teleportation or runs a quantum algorithm 'raw', that is, without doing any error correction.

Early successes

Early experimental successes in quantum computing were achieved on three experimental platforms. The earliest successful demonstrations of quantum algorithms were executions of the two-qubit Deutsch–Jozsa algorithm using liquid-state nuclear magnetic resonance. In one case, the two qubits were two hydrogen nuclei (spin up and down are the qubit logical states) in partially deuterated cytosine. The other three hydrogens in cytosine are replaced by deuterium, and therefore do not act as qubits. In the second case, the two qubits are a hydrogen nucleus and a chlorine nucleus (an uncommon isotope with spin) within a chloroform (trichloromethane) molecule. The other two chlorine nuclei in the molecule are the common spinless variety, hence not qubits. Later a variant of the Shor algorithm was first implemented by nuclear magnetic resonance in a molecule with seven qubits: five fluorine qubits and two chlorine qubits.

Processing quantum information with nuclear magnetic resonance involves four key elements: preparing the initial state, performing single-qubit gates, performing

two-qubit gates and measuring the output. To understand these processes, we should picture the molecule as comprising atoms that are bonded together by sharing electrons. Each atom comprises a nucleus and electrons, and the nucleus can either have spin, hence serving as a qubit, or be spinless, so not playing an active role in quantum information processing. Each nuclear spin is distinguished by a unique spin frequency associated with its atomic isotope and its local neighbourhood inside the molecule. This uniqueness allows each nuclear spin to be independently addressed. The spin state can be modified by a magnetic pulse with a carrier wave of the same frequency as the nucleus. The strength of the pulse determines how much the nuclear state is modified.

The single-qubit gate, which transforms a qubit into a new state, is made by applying a magnetic pulse. Two-qubit gates are created by a sequence of magnetic pulses as follows. As nuclei are coupled via the electronic bond, the frequency of one nucleus is modified by interaction with the state of the other nucleus and vice versa. Thus, the spin of one nucleus can be flipped (changing $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$) only if the other nucleus is in state $|1\rangle$ but not otherwise. A universal set of gates can be made from just two distinct single-qubit operations plus this one two-qubit operation.

A key problem with liquid-state nuclear magnetic resonance, which demonstrated so many proof-of-principle quantum computing advances, is that the molecules are warm. The molecule's multi-qubit initial state is an almost-uniform mixture of all numbers instead of satisfying DiVincenzo's initialization condition of all $|0\rangle$. A small but useful deviation from such an inauspicious initial state is achievable, leading to significant proof-of-principle experiments. However, any exponential advantage of quantum computing is washed away by the initial warm state, which is one reason that a working quantum computer is not expected to be achieved by liquid-state nuclear magnetic resonance.

3 Current directions

Leading technologies

Leaping forward to today, the leading technologies at the moment are based on ion-trap, superconducting-circuit and photonic systems. Each of these technologies has multiple approaches and which approach will win, if any, is an open bet. Other options include semiconductor quantum dots, neutral atoms in lattices, photonics and the exotic approach of Majorana fermions based on topological superconducting nanowires.

Theoretical and experimental developments are taking place in universities, major companies and rapidly growing start-up companies. Whereas universal quantum computers with fault-tolerant quantum error correction dominated technology development in the early years, nowadays many groups and companies seek to make purpose-built many-qubit computers and brazenly eschew error correction.

Ion trap qubits

We begin with studying the ion trap, which has impressive achievements under its proverbial belt. An ion trap employs radio-frequency electric fields to confine ions. These ions, as charged atoms, repel each other. Consequently, if the ions are cold enough, they form an effective crystal corresponding to an array of ions that share collective motion. The electronic energy levels inside each ion are quantized, meaning that they have discrete energy levels, and the collective motion is also quantized.

The motional state of the ion crystal is harmonic. Harmonic oscillation is ubiquitous in nature and corresponds to having an oscillation period that is independent of its amplitude. Examples of harmonic oscillation include the inductor–capacitor circuits used for radio circuits and low-angle pendulum oscillation used in grandfather clocks. An amplitude-independent frequency means that the period is robust against variations in the strength of oscillation. This desirable feature translates to the atomic scale where the frequency of an electronic transition is independent of the strength of the electromagnetic field driving the transition. Anharmonic oscillation refers to amplitude-dependent periods, exhibited by a pendulum clock with an excessive initial angle, for example.

Harmonic oscillation in the quantum regime has the property that its energy levels are discrete and equally spaced. For equally-spaced energy levels, we associate energy changes with a particle. For electromagnetic radiation such as visible light or microwave fields, we refer to the particle as a photon. For harmonic mechanical oscillation, the particle is called a *phonon*, derived from the Greek word *phonos* for 'voice'. The photon and the phonon are legitimately regarded as particles because, for a given frequency and spatial characteristic, photons are identical to each other and conserve energy and momentum during interactions and the same holds for phonons. The notions of energy and frequency are interchangeable for massless particles such as photons and phonons. The two quantities are proportional to each other, with the proportionality being given by Planck's constant.

The ionic qubit corresponds to the two lowest electronic energy levels of an ion, which are typically of microwave separation. The energy separation is known as hyperfine splitting and arises from the magnetic interaction between the electronic charge distribution and the nucleus. Although changing the qubit state could be achieved by a microwave pulse, instead two nearly resonant laser beams are used, for example in the ultraviolet region of the spectrum. The difference frequency between the beams is in the microwave regimes and this difference is used to drive the qubit transition. The advantage of using high-frequency lasers for a low-frequency transition is that these lasers can each focus on distinct ions whereas a microwave beam is too broad.

Now imagine that the two laser beams have a frequency difference that is too low or too high for the ion to notice. The gap between this laser-beam frequency difference of the laser beams and microwave frequency between the two ionic energy levels is known as detuning. To modify the ionic qubit, the detuning must be nearly zero for a stationary qubit.

However, the ion need not be stationary as the crystal of ions can move. For example, the crystal can rock back and forth. If the ion is moving, then the ion experiences a different detuning from the pair of laser beams. This motional dependence of detuning is analogous to the Doppler shift of sound waves: the pitch of a siren depends on whether the emergency vehicle is approaching you or heading away and on how fast the vehicle is moving. Through the Doppler shift, ions can absorb photons only if the photon frequency is suitably detuned from the ionic transition frequency. In this way the Doppler shift enables cooling of ions: by detuned illumination of ions, the ions can only accept photons by giving up phonons. Losing phonons decreases mechanical energy meaning the ions slow down and thus cool.

The Doppler shift also enables a two-qubit gate in a rather elegant way. Let us consider the two-ion Sørensen–Mølmer gate: two ions in the rocking linear chain are illuminated by laser beams such that the pair of beams on one ion have a negatively detuned frequency and the pair of beams on the other ion are positively detuned. Thus, one ion yields a phonon to change its electronic state while the other ion gains a phonon to change its state. If they work in tandem, the net result is no change to the mechanical motion of the rocking ion chain.

To ensure that only pairs of ions can collaborate in this way, the laser-beam pair illuminating each ion is not detuned at the rocking-chain frequency but rather slightly detuned. This slight detuning prevents one ion from changing its state through dissipating mechanical motion and ensures that two ions simultaneously change their state. For the right pulse strengths, the Sørensen–Mølmer gate effects the operation $|00\rangle$ to $|00\rangle+|11\rangle$ and $|11\rangle$ to $|00\rangle-|11\rangle$, which is a superposition of flipping both qubits and not flipping both qubits.

The two-qubit gate employs mechanical motion as well as the ion's electronic transition. This additional physical system of mechanical oscillation is used to get two possibly distant qubits to collaborate and is known as a quantum bus. The term quantum bus generalizes the notion of a bus in classical computer architecture, wherein the bus serves as an inter-component data-transfer communication system. For ion-trap quantum computing, the bus data are effectively the phonons of collective crystal motion.

The quantum algorithm begins with all ions in the ground state, executes single- and two-qubit gates to process quantum information and finishes with readout. The readout is achieved by highly efficient fluorescence imaging. This involves hitting the ion with optical pulses that cause the $|0\rangle$ state to transfer to a state that does not glow (fluoresce), whereas the $|1\rangle$ state becomes excited and does glow. A glowing ion is read as 1 and a dark ion is inferred to be 0, and the final string of bits is thereby known. The calculation is complete.

Remarkable progress has been achieved to date, making ion-trap quantum computing arguably the most advanced quantum computer technology at present. Today's ion traps can hold dozens of ions for hours and have coherence times that are longer than thousands of seconds. Seven or eight qubits can be operated in a fully connected way, which means that a two-qubit gate can be applied to any pair of ions. Single-qubit gates can be executed on a microsecond timescale. Preparation

and readout both can be done with fidelities of better than 0.999 where a fidelity of 1 signifies perfection.

Superconducting qubits

Superconducting technology offers another exciting pathway for creating quantum computers. It is the focus of most industrial research efforts, both within large companies such as Google and IBM as well in start-up companies such as D-Wave Systems and Rigetti. Superconducting quantum computers have the advantage of being solid-state systems, which means that they do not suffer much from the loss of qubits that is such a hindrance for atomic quantum computing including ion-trap technology. Whereas coherence is a major problem for solid-state semiconductor-based quantum computing, such as quantum-dot implementations, superconducting implementations have good coherence times. On the other hand, superconducting systems operate at extremely low temperatures, making them complicated and expensive to run.

The concept of superconducting quantum computing is to create a network of connected artificial atoms rather than a network of natural atoms, as in an ion trap. Each artificial atom is realized as a nonlinear inductor–capacitor circuit. Without a nonlinear element in the circuit, the inductor–capacitor circuit is harmonic so the energy levels are equally spaced. An artificial atom must have the property that transitions between pairs of energy levels can be separately addressed, which can be done if energy separations between pairs of levels all differ from each other.

The superconducting qubit can be operated in different parameter regimes and with different circuit geometries. Circuit types vary in terms of what property is quantized and have names such as Cooper-pair boxes, quantronium, transmons, phase qubits, flux qubits, fluxonium and xmons. A superconductor enables an electric current in a circuit loop to circulate without resistance. The electric field oscillates with a characteristic frequency that depends on the product of the inductance and the capacitance of the electric circuit. The electric current experiences no resistance during its oscillation and is dubbed a supercurrent.

A clockwise supercurrent generates a downward magnetic flux and a counter clockwise supercurrent generates an upward magnetic flux. For a sufficiently small system, the magnetic flux is quantized and, as a harmonic system, the flux levels are equally spaced. Superposing clockwise and counter-clockwise supercurrents creates a superposition of up and down magnetic fields.

For a small circuit, the magnetic flux is quantized and equally spaced apart, which is not helpful for making a two-level qubit. To make the spacing unequal, a Josephson junction is placed into the circuit. A Josephson junction comprises two superconducting materials weakly linked via another medium such as an insulator. The supercurrent going around in a loop encounters an energy barrier at this weak link and this modifies the otherwise harmonic supercurrent oscillation to an anharmonic dynamic.

Anharmonicity results in unequally spaced magnetic flux levels. For sufficiently high anharmonicity, just the two lowest levels play a role in the dynamics so we have

an effective two-level atom that functions as a *flux qubit*. The downward magnetic flux serves as $|0\rangle$ and the upward flux as $|1\rangle$.

A *charge qubit* is created by a supercurrent in a loop with a low Josephson-junction charging energy. In this case, a superconducting-circuit is a qubit with a Cooper pair of electrons on the left ($|0\rangle$) or right ($|1\rangle$) of a Josephson barrier. The Cooper-pair box is a type of charge qubit and involves a superposition of two different charge states. The transmon is an enhanced version of a Cooper-pair box with a greater ratio of Josephson-junction energy to charging energy in order to reduce the deleterious effects of charge noise. A disadvantage of transmons is that weak anharmonicity means that additional levels beyond the two levels required for qubit operation can affect performance. This can be managed through clever control techniques.

Both flux and charge qubits are promising media for quantum-computer technology. Flux qubits and transmons, and their variants, are currently favoured in industrial efforts to build a quantum computer. Each of the qubit types has advantages and disadvantages. D-Wave Systems works with a variant of flux qubits that include extra magnetic-flux loops to enable tuning frequencies so that the flux qubits are effectively identical. In D-Wave computers, thousands of flux qubits are arranged into a two-dimensional array, which can be regarded as an array of magnetic dipoles that are only free to point up or down or in superpositions of up and down.

Flux qubits interact via couplers, which are themselves superconducting loops, hence magnetic dipoles. We can regard the computer as being a vast array of coupled magnetic dipoles with some magnets being bits and some magnets being the mechanism to couple bits together. The complexity of the array is further complicated by the inclusion of control circuitry to modify dynamically the qubit parameters and couplers. Studies suggest that the D-Wave Systems computer exhibits entanglement within subsets of qubits over part of the computational runtime. However, the computer has not yet demonstrated a computational speedup over a classical computer running the best-known algorithm for the computational problem at hand.

The IBM Experience, on the other hand, uses transmons for qubits. This cloud-based quantum computer initially had five qubits but this has been increased to 16 qubits. Singe-qubit gates are achieved by directly driving charge-qubit transitions in the transmon, whereas two-qubit gates are mediated by microwave photons in a resonator. Transmons behave like electric-dipole antennas and therefore couple strongly to the resonator. The resonator serves as a quantum bus, and the role of the resonator photons is analogous to that of crystal motion in ion-trap quantum computing.

Photonic qubits

Both ion-trap and superconducting quantum computing involve atoms or artificial atoms manifested in a matter system, but quantum computing is also possible with photons acting as qubits. The two logical states of the qubit can be manifested in

various ways such as whether the photon is present or not (single-rail qubit); which of two paths the photon is travelling (dual-rail qubit); which of two polarization states the photon is in (polarization qubit); or whether the photon is arriving early or late (time-bin qubit). Photonic qubits are important not just for quantum computing but also for quantum communication protocols such as quantum key distribution.

Photonic qubits are typically prepared in one of two ways: with spontaneous parametric down conversion or with a single natural or artificial atom confined in some way. Spontaneous parametric down conversion produces a correlated pair of photons simultaneously but at a random time. Thus, when and where the photons are must be treated as being indeterminate. Furthermore, pairs of pairs of photons and sextuples and higher-order terms are created with diminishing probability. Unlike matter qubits, which have mass and perhaps charge and thus are easy to locate and count, the number of photonic qubits is indeterminate. This indeterminacy leads to computational errors that must be ameliorated.

One way to manage indeterminacy of photons is to detect one of two correlated photons and thereby presage detection of the other photon, with the where and when of detection constrained by energy and momentum conservation laws. The photon sacrificed to find the other is known as a herald because this photon announces the existence and properties of the other photon. For quantum computing, many photons are required, each serving as a qubit, plus their partner photons serving as heralds for these qubits. In experiments, the aim is to perform multiphoton coincidence measurements whereby many detectors clicking at the same time reveal both the herald photons and the bit-string output. The latter is constructed by measuring in which of two possible output states each computational photonic qubit is found.

Although effective in rooting out some errors due to qubit-number indeterminacy, the randomness of photon-pair creation times leads to success probabilities that fall exponentially with the number of photons being used. This exponential drop in success probability removes any exponential advantage that quantum computing could provide. This problem must be fixed if photonic quantum computing is to become valuable.

One way to improve single-photon sources is to employ a natural or artificial atom, such as a quantum dot. If such an atom behaves like the two-level system discussed above, then a laser-pumped atom can only emit one photon before it can recover and re-excite. Thus, the atom can behave like a photonic machine gun, firing a sequence of photons that can be used for photonic quantum computing. However, the photon emission is omnidirectional in free space, as though the marksman holding the photonic machine gun fires in random directions. This problem can be partly removed by coupling the atom to a resonator, as we discussed in a different context for the transmon coupled to a resonator. The photons emitted from the atom then have a preferred direction and are then useful for quantum computing.

Unfortunately, the photon machine gun is not yet efficient, behaving as though most of the photonic bullets are blanks. The probabilistic nature of photon generation contributes to an exponential overhead for obtaining multiphoton coincidences that answer computational problems so has the same problem as using

spontaneous parametric down conversion. However, strategies exist to compensate for high qubit loss rates, even up to half of the qubits getting lost under certain conditions and for specific ways to perform quantum computation.

Making qubits is the first step; processing with a universal set of gates is second. Single-qubit gates are performed with standard linear optics. Processes include rotating the polarization of light using a birefringent crystal or splitting a photon at a beam splitter that is a half-silvered mirror. Technical challenges include aligning all the beams so that photons arrive at the correct angle and with the right timing to avoid errors. Conceptually, however, single-qubit gates are straightforward to understand.

The two-qubit gate is a major challenge for photons. The enticing way to achieve a two-qubit gate is to exploit what is known as an optical Kerr nonlinearity. In linear optics, light is slowed and bent in a transparent medium such as water or glass. The light still gets through the medium but deviates from its original destination and arrival time by the polarizing effect of the medium. In fact, some loss of light occurs during passage through the medium, and the amount of loss is tied to the amount of the light beam's deviation; this locked relationship between deviation and loss arises from the principle of causality, which prevents the future from affecting the past.

The optical Kerr nonlinearity causes deviation and delay that depends on the strength of light present in the medium. In the extreme case of a single-photon nonlinearity, the path of a single photon of light could deviate if a second photon in another beam path is present and not deviate if this second photon is absent. Following the principle that every action causes an equal and opposite reaction, this second photon would deviate if the first photon were present and not otherwise. If each photon serves as a dual-rail qubit in the photonic quantum computer, then quantum information is encoded into the path of each photon, and a path deviation occurs only if both photons are in a mutually colliding path. This state-dependent change to both photonic qubits suffices to realize a two-qubit gate, and a universal set of quantum logic gates is realized.

Unfortunately, the optical Kerr nonlinearity is weak, lossy and distorts the photon pulse, making this two-qubit gate a pipe dream for now. One way to circumvent the problem is to slip the photon into an optical resonator (analogous to the microwave resonator discussed in the context of transmon-based superconducting quantum computing) and deploy the weak nonlinearity over a long time while the photon is inside. However, the conversion of the photonic qubit from a freely propagating pulse to an intra-resonator field is not easily reconcilable with the requirements of photonic quantum computing. Although still a possibility for optical quantum computing, the bets on photonic quantum computing are currently on linear optical approaches.

That linear optics suffices to replace the nonlinear optical Kerr effect is surprising and based on the notion of quantum teleportation. Quantum teleportation aims to transmit quantum information from one point to another through a channel, or route, that destroys quantum information. If two parties at two different points share prior entangled states, the party at one point jointly measures the (unknown) quantum information and the share of the entangled state at that point. She then

transmits the measurement result to the party at the other point who uses the received information to transform his share of the entangled state to a replica of the original (unknown) quantum information. The idea of teleportation is that entanglement and communication of classical information can replace the need for a quantum channel connecting the two points.

In quantum teleportation, quantum information is simply destroyed at one point and replicated at another point, consuming prior entanglement and classical communication bandwidth in the process. However, instead of replicating the quantum information, we want the quantum information appearing at the second site to be processed by a quantum logic operation instead. The Gottesman–Chuang teleportation protocol shows how teleportation can incorporate certain logic operations, and the two-qubit photonic gate is one such example.

Instead of trying to perform an infeasible two-qubit optical gate, the Knill–Laflamme–Milburn linear optical quantum computing concept proposes preparing entangled states in advance that can be used to execute the gate. Moreover, this entanglement resource can be prepared using linear optics in a heralded way. Sometimes the right state is produced, sometimes not, but when the right state is produced, the right state is heralded and stored in optical quantum memory and subsequently injected into the quantum computer at the proper time to achieve the desired two-qubit gate. A universal set of gates is thus achieved.

Although the Knill–Laflamme–Milburn concept is beautiful, it is not practical. Fortunately, several great ideas followed that moved optical quantum computing to a plausible implementation and, in fact, a start-up company currently in stealth mode is developing photonic quantum computing. The key development that makes photonic quantum computing viable is that a source of few-photon entangled states, comprising nondeterministic single-photon sources, can be made near-deterministic by heralding and then mixed together via linear optics to produce a special entangled state. This special entangled state serves as a universal quantum computing state: a suitable sequence of single-photon measurements can perform any computation including those for which a quantum computer delivers a speedup. This procedure is tolerant of high photon loss rates.

Topological qubits

Now we have considered qubits as charged atoms, as artificial atoms in superconducting materials, as nuclei and as photons. Each of these qubit manifestations is local: each qubit can be thought of as occupying some region of space at some interval of time. A totally different kind of qubit is also possible, known as a topological qubit.

We are used to particles being of two types: bosons, for which the quantum state is unchanged under two-particle exchange, and fermions, for which the quantum state changes sign under two-particle exchange. Fundamental matter, like electrons, quarks and neutrinos, are fermions, and fundamental quantum fields like electromagnetism and the weak and strong nuclear forces, are constructed from bosons. In two-dimensional space, another type of particle can exist, called anyons, with the

'any' root of 'anyon' referring to the freedom to acquire any unit-modulus complex number under exchange of any two particles. A topological quantum computer can be conceived where the qubits are constructed from anyons and the quantum logic gates are obtained through anyon braiding, i.e., winding anyons around each other.

Although a quantum computer in a two-dimensional Universe seems like science fiction, a real-world topological quantum computer is plausible. In fact, Microsoft invests in this direction for constructing quantum computers, which require semiconductor and superconductor components plus a magnetic field to produce a topological superconductor. Great progress has been made towards realizing the topological superconductor, known as a Majorana nanowire, but neither the anyon qubit nor the braiding operations have been unambiguously demonstrated so far. On the other hand, the expected robustness of topological quantum computing against errors makes this research direction well worth the effort.

4 Outlook

Rapid progress

Quantum computing technology has evolved remarkably since the concepts were developed in the 1980s and serious proposals for implementations were first made in the 1990s. Early realizations of qubit strings, quantum information processing and readout were performed in universities and fundamental research laboratories in companies. Today, quantum computing technology is developed in both academic and industrial laboratories, and industrial activity involves both large corporations and small, brazen start-ups alike.

Little consensus exists regarding which medium is most promising. Companies are working on superconducting, ion, photon and anyon qubits and their deployment for quantum computing. Even within one of these technology endeavours, consensus has not yet formed on which qubit is the best. Superconducting quantum computing is undertaken with both flux qubits and transmons. Ion-trap quantum computing involves various choices of atoms. Although decades old, quantum computing technology is still at an early stage so the winning technology, if any, is not known.

Architectures and algorithms

Current quantum computer technology deploys on the order of 10 qubits. Proper state preparation, processing and measurement are achieved but not yet up to the requisite standards for scaling the size in a fault-tolerant error-corrected way. On the other hand, great enthusiasm exists for elevating the size of systems beyond 50 qubits with gates that perform even better than those available today. Whether 50-qubit systems with high-fidelity quantum gates suffices to beat classical computing is unknown, but a lot of great physics and perhaps some algorithmic advances will ensue from these courageous endeavours.

One exciting potential for extracting more power from quantum computing than currently expected relies on developing sound computer architectural principles for quantum computing. Currently the focus is on building better components such as

superior preparation and measurement of qubits and better-functioning gates. On the other hand, the value of quantum computing emerges from performing a given task, such as running an algorithm, at the threshold performance level for the task to be accomplished. Perhaps an excellent gate is needed in one part of the circuit and a worse gate can be tolerated elsewhere. Maybe one part needs error correction more than another part.

Allocating resources in the form of great qubits and gates, or deploying fault-tolerant error correction in some places and not others, could enable the quantum computer to extract more quantum-enhanced computational power than if quantum resources were equally deployed throughout. Whether smart architecture and clever quantum compiling based on sophisticated co-design principles can help is not yet known, but these approaches have the potential to accelerate the development of quantum computing.

At the component level, better understanding of the environment and superior quantum-control procedures are likely to lead to superior preparation, processing and measurement as well as more realistic assessments of how much error correction is needed to execute a given algorithm successfully. As some quantum algorithms are only meant to give guesses that can be efficiently checked on a classical computer, some sacrifice of quality that leads to poorer guessing could be an acceptable price to pay. Improved entangled-state generation could provide a viable substitute for some hard-to-realize gates.

Outperforming classical computers

Given that ideal quantum computers with up to 45 qubits can be simulated today and this number of qubits could increase slightly soon, quantum computers should have at least 50 qubits to exceed classical simulation capability. Classical computer simulations of 45-qubit quantum computation have the advantage of providing direct techniques to verify and validate the performance of the quantum computer and also provide a lower bound on what the target size should be for a useful quantum computer.

The target size of a useful quantum computer is not yet known because the minimum number of qubits, operating under imperfect conditions to execute a useful algorithm, is not known, but candidate algorithms for quantum chemistry and optimization are being studied. Whether quantum computing can outperform classical computing and whether a useful problem needs a quantum algorithm to be solved remain outstanding problems, but one point is clear: quantum computer technology is rapidly advancing and will continue to do so for the next few years and beyond.

Additional resources

- Special Issue: Quantum Information Processing *Science* **339** 1163–84 (2013); Recent articles summarizing state of the art for building a quantum computer.

- Aaronson S 2013 *Quantum Computing Since Democritus* (Cambridge: Cambridge University Press); popular book on quantum computing by a leading computer scientist.
- Brown J 2000 *Quest for the Quantum Computer* (New York: Simon & Schuster); early popular book about quantum computing, written by a science journalist.
- Deutsch D 1985 Quantum theory, the Church–Turing principle and the universal quantum computer *Proc. R. Soc. London* A **400** 97–117; seminal paper motivating quantum computing and presenting principles for building a quantum computer.
- Dowling J P 2013 *Schrödinger's Killer App: Race to Build the World's First Quantum Computer* (Boca Raton, FL: Taylor & Francis); popular, humorous book on quantum computing and its important applications by a leading physicist.
- Feynman R 1982 Simulating physics with computers *Int. J. Theor. Phys.* **21** 467–88; transcript of a seminal lecture motivating quantum computing given by an outstanding physicist who is also a gifted communicator.
- Kaye P, Laflamme R and Mosca M 2007 *Introduction to Quantum Computing* (Oxford: Oxford University Press); introductory textbook suitable for senior undergraduates in physics or mathematics.
- Lloyd S 2006 *Programming the Universe: A Quantum Computer Scientist Takes on the Cosmos* (New York: Knopf); popular book, written by a leading quantum computing expert, on quantum computing, which raises profound questions and speculation.
- Mermin N D 2007 *Quantum Computer Science* (Cambridge: Cambridge University Press); introduction to quantum computing suitable for a senior undergraduate.
- Milburn G J 1999 *The Feynman Processor: Quantum Entanglement and the Computing Revolution* (Reading, MA: Basic Books); early book on quantum computing written by a leading physicist.
- Nielsen M A and Chuang I L 2010 *Quantum Computation and Quantum Information: 10th Anniversary Edn* (Cambridge: Cambridge University Press); the most popular textbook on quantum computing.
- Rudolph T 2016 Why I am optimistic about the silicon-photonic route to quantum computing arXiv:1607:08535; well written article by a leading quantum information scientist arguing that photonic quantum information processing is promising.
- Stolze J and Suter D 2004 *Quantum Computing: A Short Course from Theory to Experiment* (Weinheim: Wiley-VCH); textbook on quantum computing.