AU J.T. 13(3): 151-157 (Jan. 2010)

Quantum Computing

David Tin Win

Faculty of Science and Technology, Assumption University
Bangkok, Thailand
E-mail: <dtwin@email.com>

Abstract

A description of the general principles of quantum computing is followed by a discussion of different quantum concepts, advantages, applications and documentation describing the leading scientists and institutions at the forefront in exploiting the laws of quantum physics governing subatomic particles for building a faster and more efficient computer.

Keywords: *Superposition, quantum physics, subatomic particles, qubit, quantum dot, spintronic transistor, chemical computer.*

Introduction

Electronics are shrinking. This creates challenges on the limits of the ability to craft increasingly tiny features. These features etched with extremely high-energy laser light are processor components. Disk drives store information in ever-smaller clusters of atoms. Major inhibitions are electrical, magnetic, and quantum interferences that set limits to how many transistors can fit into a given finite volume. According to Moore's Law, the density of integrated chips should double every six months (Gershenfeld and Chuang 1998). It will become ever more difficult to maintain and detect signals such as the state of a memory bit. To circumvent these, scientists are exploring the possibility of molecular memory or information storage in chemical structures of single molecules.

The origins of quantum computing are not too far back. It was first theorized less than 30 years ago, by a physicist at the Argonne National Laboratory. Paul Benioff was the first to apply quantum theory to computers in 1981. He theorized about creating a quantum Turing machine. Most digital computers are based on the Turing Theory (Bonsor and Strickland 2009).

Molecular memory requires chemicals that can oscillate between two stable states, just like atom clusters switching magnetic states on disk drive surfaces. Most of these molecular switches involve structural changes. When changing states, large molecular chunks move relative to each other. However a flat molecule (eg. naphthalocyanine) can change states without undergoing any structural changes. Structurally identical molecules with different conformation are called tautomers. The process is called tautomerization. The memory states can be changed and read through the same technique used in electronics today: changes in electrical conduction (Timmer 2007).

A team of European researchers were able to induce the hydrogens in naphthalocyanine (shown in Fig. 1) to swap locations: single-molecule storage. A tunneling microscope pushed several naphthalocyanine molecules close enough to form linked orbitals.

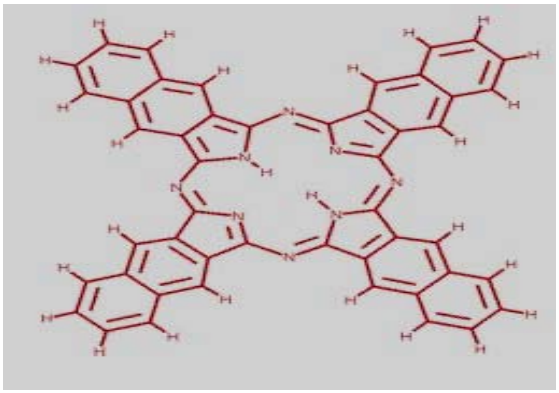

Fig. 1. Naphthalocyanine, a flat molecule. It can change states without any structural changes – tautomerism (Timmer 2007).

Different members of the structure can be selectively switched, depending on the position where current is injected in the rings. It was suggested that similar arrangements can be employed for coordinated switching of atomic bits and enabling the state of one bit to influence the response of its neighbors (Timmer 2007).

Some scientists are now exploring quantum computing, using a computation device where direct use of quantum mechanical phenomena (superposition and entanglement) is made to perform data operations. The fundamental principle is that data can be represented by quantum properties that can be used to perform operations on these data. Quantum computers are different from other computers such as DNA computers (uses DNA, biochemistry and molecular biology) and traditional computers based on transistors (Wikipedia 2009). An interesting development is the *chemical computer*. Also called reaction-diffusion computer or BZ (Belusov-Zhabotinsky) computer, it is an unconventional computer based on a semi-solid chemical mixture. The data is represented by varying chemical concentrations. The computations are performed by naturally occurring chemical reactions. It is in a very early experimental stage (Wikipedia 2009).

Quantum Computers

Quantum computing is an effort to harness the bizarre laws that operate in the sub-atomic world into practical devices that would revolutionize the speed at which information is shared and processed. Scientists say they have taken a big step forward towards the development of quantum computing, a process they believe could form the basis of a new form of internet that would work at the speed of light (ABC 2009).

Bits are memory components of classical computers. Each bit holds either a one or a zero. The corresponding memory components in a quantum computer are qubits. The memory has a sequence of qubits. A single qubit can hold a one, a zero, or a quantum superposition of these two, just like music notes of different frequencies forming harmonics. Generally a quantum computer with n qubits can simultaneously be in up to 2^n different states. For example a pair of qubits can be in a quantum superposition of 4 states. Three qubits can exist in a superposition of 8. This is in contrast to a normal computer that can only be in *one* of 2^n states at any given time. On operation a quantum computer manipulates those qubits with a fixed sequence of quantum logic gates. The sequence of gates used is a *quantum algorithm* (West 2000).

The state of a classical computer operating on a three-bit register has a probability distribution over the $2^3 = 8$ different three-bit strings 000, 001, ..., 111 at any time. Thus it is described by eight nonnegative numbers (a, b, c, d, e, f, g, h), which add up to one.

Similarly the state of a three-qubit quantum computer is described by an eight-dimensional vector (a, b, c, d, e, f, g, h) – a wave function. But the constraint here is that the sum of the *squares* of the coefficient magnitudes, $|a|^2 + |b|^2 + ... + |h|^2$, must equal one. In addition, the coefficients being complex numbers can be negative as well as positive. This allows for cancellation, or interference, between different computational paths. This is a key difference between probabilistic classical computing and quantum computing (Wikipedia 2009).

It is easily seen that there are many different possible ways of specifying an eight-dimensional vector, depending on the basis chosen for the space. The basis of three-bit strings 000, 001, ..., 111 is known as the computational basis. Other bases like unit-length and orthogonal vectors can also be used. Ket notation is used to show explicit basis choice.

For example, the state (a, b, c, d, e, f, g, h) in the computational basis can be written as

$$a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle,$$

where $|010\rangle$ = (0,0,1,0,0,0,0,0), etc… The computational basis for a single qubit in two dimensions is $|0\rangle$ = (1,0), $|1\rangle$ = (0,1), but another common basis is the Hadamard basis of $|+\rangle = (1/\sqrt{2}, 1/\sqrt{2})$ and $|-\rangle = (1/\sqrt{2}, -1/\sqrt{2})$.

Any system with an observable quantity *A*, *conserved* under time evolution and has at least two discrete and sufficiently spaced consecutive eigenvalues may be used for implementing a qubit (Carey 2002). This is because such systems can be mapped onto an effective spin-1/2 system. One of the key principles that support the concept is that quantum mechanics allows atomic particles to exist in two states simultaneously. Thus the quantum mechanical states of an atom may be used to represent information and make quantum computers very much more useful for complex calculations than conventional one/zero or on/off computer bits (Barenco 1996). Another mind-bending aspect is that the quantum state atoms can be linked to other atoms, regardless of how far apart they are. Changing one changes the other automatically. Recently (January 23, 2009) scientists reported the instantaneous teleportation of information between two unconnected atoms that are one metre apart (ABC 2009).

A simple example of qubits for a quantum computer is the use of particles with two spin states. The spin of an electron can be in one of two spin states characterized by spin quantum numbers: (+1/2) and (-1/2) in units of $\hbar$ (= $h/2\pi$; where h is Planck's constant). Alternatively, these are "up" and "down" spins; or clockwise and anticlockwise spins written in the ket notation as $|\uparrow\rangle$ and $|\downarrow\rangle$, or $|0\rangle$ and $|1\rangle$.

Quantum Decoherence

Quantum decoherence is the mechanism involved in the interaction of quantum systems with their environments, with consequent exhibition of probabilistic additive behavior. It gives the *appearance* of wave function collapse. It prevents system and environment wave function's different elements in the quantum superposition from interfering with each other.

Removing or controlling decoherence is one of the greatest challenges. Generally this means isolating the system from its environment. Otherwise any slight interaction with the external world would cause system decoherence. This effect is irreversible and should be avoided, or highly controlled.

Candidates

The following are some candidates for quantum computing:

- Superconductor-based quantum computers (including SQUID-based quantum computers);
- Trapped ion quantum computer;
- Optical lattices;
- Topological quantum computer;
- Universal quantum automaton;
- Quantum dot on surface (e.g., the Loss-DiVicenzo quantum computer);
- NMR on molecules in solution (liquid NMR);
- Solid state NMR Kane quantum computers;
- Electrons on helium quantum computers;
- Cavity quantum electrodynamics (CQED);
- Molecular magnet;
- Fullerene-based ESR quantum computer;
- Optic-based quantum computers (Quantum optics);
- Diamond-based quantum computer;
- BEC-based quantum computer;
- Transistor-based quantum computer - string quantum computers with entrainment of positive holes using a electrostatic trap;
- Spin-based quantum computer;
- Adiabatic quantum computation;
- Rare-earth-metal-ion-doped inorganic crystal based quantum computers.

This large list of possible candidates shows that the topic is still in its early stages.

Quantum Computing in Computational Complexity Theory

Current mathematically known factors about the power of quantum computers are surveyed here. Known results from computational complexity theory and the

theory of computation dealing with quantum computers are mentioned.

"Bounded error, quantum, polynomial time" BQP is defined as the class of problems that can be efficiently solved by quantum computers. Quantum computers only run probabilistic algorithms, so BQP on quantum computers is the counterpart of BPP on classical computers. BQP is the set of problems solvable with a polynomial-time algorithm. The error probability is bounded away from one quarter. A quantum computer "solves" a problem if its answer is right with high probability every time. If the solution is in polynomial time, then BQP contains the problem.

BQP is in the complexity class #P (or more precisely in the associated class of decision problems $P^{\#P}$), which is a subclass of PSPACE (see Fig. 2).

BQP is believed to be disjoint from NP-complete and a strict superset of P. Both integer factorization and discrete log are in BQP. Both of these are NP problems believed to be outside BPP, and are therefore outside P.

Quantum computers are faster than classical computers; however those listed above are unable to solve any problems that classical computers cannot solve. A timeline of computer computing is shown in Wikipedia (Wikipedia 2009).

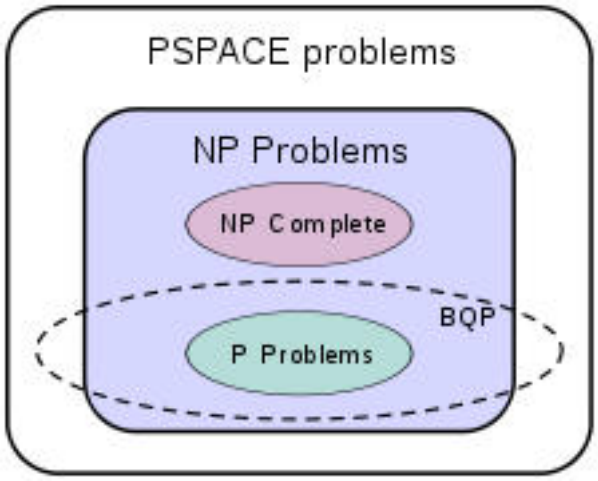

Fig. 2. The suspected relationship of BQP to other problem spaces (Wikipedia 2009).

Current Research

There are many institutions that are involved in the field of quantum computing, both private and government. In the last decade interest in quantum computing has mushroomed. The first big breakthrough in constructing a computer that behaved according to the laws of quantum physics arose in the early 1980's when Richard Feynman, California Institute of Technology, Nobel Prize winner, reasoned that the only way a system could exist which allowed particles to spin clockwise and counterclockwise simultaneously was to have a computer that behaved the same way. This early idea of symmetry between a quantum mechanical system and a computer led to the next big breakthrough in 1994 by a scientist named Peter Shor at Bell Laboratories in New Jersey. He presented the first algorithm demonstrating theoretically how a quantum computer could quickly reverse-factor large numbers. This interested the United States Federal Government because the codes that protect military and financial secrets are based on the inability to do such reverse factoring.

MIT and Los Alamos National Laboratory

(Gershenfeld and Chuang 1998)

In March 1997, quantum computing was brought one step closer when addition of two numbers was performed by using Nuclear Magnetic Resonance to flip the nuclear spins of the organic molecule, alanine – an alpha amino acid. The atoms were then embedded within a large molecule and used the direction of their spins to represent data. In detail, the core of the experiment was a tiny amount alanine or actually the trillions of atoms within. This was possible because in this sample of atoms, most are found pointing in any random direction. However a very small percentage was found pointing in a specific direction.

The spins of the randomly pointing atoms cancel each other. This allows an NMR machine to recognize the small percentage of atoms that are pointed in the same direction.

These atoms that are found in plurality constitute one quantum bit, or qubit.

The alanine molecule yields three qubits because it has 3 atoms of carbon that each correspond to a different NMR frequency, and the atoms are also linked in a manner that they could be used for addition. The scientists used two of the carbon atoms to accomplish the addition of one and one. In this experiment, the hardware was the atoms, and the software was the radio pulse used to manipulate the atoms. "Each pulse made one atom in the pair (the "target") shift the orientation of its spin, in a way that depended on both the duration of the pulse (say one-hundredth of a second for a quarter turn) and on the orientation of the partner atom, the "control". When the program was finished, the final spin state of the atoms, gave the answer- two, in this case" (Hogan 2003). The ability to apply this concept to sorting, picking a telephone number from a list of four other numbers was mentioned (Hogan 2003).

University College London

(Hogan 2003)

Making quantum computers practical is the goal of University College London materials scientist Marshall Stoneham. He received £3.7 million to produce a quantum device that calculates efficiently, functions at higher temperatures than competing machines, and can be assembled with existing equipment.

Current quantum computers can store and manipulate quantum bits (qubits) either by exploiting an ion's energy state or using the spins of atomic nuclei to represent 0 or 1. However, ion manipulation approach on a quantum computer requires it to be extremely large; a nuclear-spin-based device requires magnets cooled by liquid helium. The latter cannot handle qubit increases past a certain point as the noise from neighboring molecules can mask the resulting signal.

A design for a silicon-based quantum computer was proposed by an Australian researcher Bruce Kane (Hogan 2003), who theorized that phosphorus-impregnated silicon could yield a device that stores qubits in the spins of the embedded atoms' nuclei. The spins could be flipped by radio signals, and the neighboring atom interactions could be followed by an electrode. This would enable linked qubits to perform operations. Such a design could supposedly contain thousands of qubits that would be manipulated by existing electronics.

Stoneham (Hogan 2003) proposed to manipulate electron spins rather than nuclear spins. Embedded atoms are to be randomly distributed within the silicon and laser light is to be employed to manipulate electron spin. Qubits would be connected with "control atoms" that can be excited by specific laser-light frequencies, just like the qubit electrons (Hogan 2003).

The Institute for Microstructural Science in Ottawa, Canada

(Burkard 2000)

Researchers built a spintronic transistor that plays a major role in the quest for quantum computing. Although simple spintronic devices such as diodes have already been created, the transistor is the first to use electron spin to control current that passes between gates. The transistor made from a "**quantum dot**", a tiny semiconductor, acts as a gateway that controls electrons by blocking them or letting them pass. This allows the storage of information that also can be read and erased by manipulating spin inside the dot (Burkard 2000).

University of Michigan

(Steeh 2003)

An important milestone on the way to creating viable quantum computers, laser-cooling of individual atoms, have been demonstrated. Christopher Monroe (Steeh 2003) stated that quantum computers using individual atoms for information storage require special conditions, such as keeping the atoms cool and electronic suspension in a vacuum. The experiment conducted at the Michigan University used electronic fields to

confine a crystal of two atoms (each a different isotope of the same element). The quantum computing atom was cooled to almost absolute zero through direct laser cooling of its neighboring atom. This process removes unwanted motion in the atom crystal without affecting the internal state of the other atom; an important step in scaling a trapped atom computer with information qubits stored in the quantum states of individual atoms.

Based on the cooling experiments, Monroe and two colleagues, David Kielpinski of MIT and David Wineland of the National Institute of Standards and Technology (Steeh 2003) proposed a quantum computer architecture model. They described a "quantum charged-coupled device" (QCCD) composed of many paired atoms connected through electrical charges of invisible "springs" and is scalable to large numbers of qubits (Steeh 2003).

Applications

The applications for quantum computing are endless. Computer systems that are capable of simultaneously processing billions of data bits would revolutionize every area of science and mathematics. It would be possible to parse in minimal time, enormous amounts of information organized in databases. Boeing has interest in preventing eavesdropping or jamming of aircraft electronic signals by using quantum computers. Another area is super accurate calibration in time keeping and satellite positioning.

As with any radically new technology, governments are strongly interested in terms of national security. A computer with this processing power level could reverse factor any level of modern encryption in real time, as well as create levels of encryption unfactorable by current computing systems.

Biochemists are interested in high performance computing to simulate protein folding after generation in cells. It would then be possible to change the individual amino acids in the protein and also alter its shape, consequently modifying how the protein acts. This would be vital in developing new drugs (Lerner 2001). One interesting progress in this direction is the IBM BlueGene project (Win 2007). Apart from these, answers to many questions in many areas of physics, chemistry, mathematics and most other areas of science, would become available.

Limitations

Can practical quantum computers of useful size be actually built in our universe? Are the theoretical constructs, the physics of quantum mechanics and our concept of the algorithms that run them entirely correct? These are nagging questions. There is no agreement yet about the best way to build a quantum computer. For example Chuang and Gershenfeld experiments at MIT used atoms or charged ions in an electromagnetic trap. But IBM tested superconducting materials that can generate quantum bits.

For quantum computers to live up to the expectations, a quantum computer capable of 100,000 calculating atoms would be required. The ultimate limitation with quantum computing is making it practical. Creating the conditions for Nuclear Magnetic Resonance, employing laser light or the need for magnets cooled by liquid helium to control electron spin, are still limiting factors.

Conclusion

Quantum computing has the future potential to reinvent not only computers, but most fields of science. At the moment it is thought of as a "scary science," because it represents things that are not fully understood yet and could open doors of scientific understanding that is unprecedented.

Scientists are now able to perform mathematical computations through controlling the spin states of an electron within an atom or molecule. By information actually being stored at a subatomic level, quantum computing will achieve unprecedented speed in processing power, capable of processing billions of bits of information at once.

When the ultimate limitation of making it practical is overcome, quantum computing will reinvent entire fields: including cryptography, engineering, weather, space flight and mathematics.

Will a quantum hyper-computer take over the world? Will it simulate a human being? Is there a possibility of it becoming a power-hungry despot that can enslave the whole world. Who knows?

References

ABC. 2009. US scientists move toward speed-of-light Internet. Australian Broadcasting Corporation (ABC). Available: http://www.abc.net.au/news/stories/2009/01/23/2473402.htm.

Barenco, A. 1996. A short introduction to quantum computation. CQC introductions: Quantum computing. Available: http://www.qubit.org/library/intros/comp/comp.html.

Bonsor, K.; and Strickland, J. 2009. How quantum computers work. Available: http://www.computer.howstuffworks.com/quantum-computer.htm.

Burkard, G. 2000. Spintronics and quantum dots for quantum computing and quantum communications. University of Basel, Switzerland. Available: http://theorie5.physik.unibas.ch/qcomp/qcomp.html.

Carey, D. 2002. Quantum computing FAQ. Available: http://www.rdrop.com/~cary/html/quantum_c_faq.html.

Gershenfeld, N.; and Chuang, I. 1998. Quantum computing with molecules. MIT. Available: http://www.media.mit.edu/physics/publications/papers/98.06.sciam/0698gershenfeld.html.

Hogan, J. 2003. Computing: Quantum bits and silicon chips. Nature 424(6948): 484-6.

Lerner, E.J. 2001. Cellular architecture builds next generation supercomputers. IBM Think Research. Available: http://www.researchweb.watson.ibm.com/20010611_cellular.shtml.

Steeh, J. 2003. Michigan researchers achieve quantum entanglement of three electrons. Univ. Michigan, Ann Arbor, MI, USA. Available: http://www.eurekalert.org/pub_releases/2003-02/uom-mra022603.php.

Timmer, J. 2007. Shifting atoms in single molecules memory. Available: http://www.arstechnica.com/news.ars/post/20070902 –shifting-atoms-in-single-molecule-memory.html.

West, J. 2000. The quantum computer - An introduction. Available: http://www.cs.caltech.edu/~westside/quantum-intro.html.

Wikipedia 2009. Quantum computing. Available: http://www.en.wikipedia.org/wiki/Quantum_computing.htm.

Win, D.T. 2007. The IBM BlueGene (Supercomputer) project - Capability in science applications (Molecular dynamics and protein folding). AU J.T. 10(4): 237-47.