QUANTUM COMPUTING: A REVIEW FOR THE RELATED ISSUES AND ITS FUTURE ASPECTS

Shubhangi Tyagi[1], Harshita Malhotra[2], Deepali Bhatia[3], Prashant Vats[4]
[1,2,3,4] *Dept. of CSE, HMRITM, New Delhi (India)*

ABSTRACT

In this paper we have carried out a review of the quantum computing technology & issues related to it. We have discussed various issues that are related to this technology. We have also reviewed the various future aspects related to this technology.

Keywords: Quantum Computing, Qubit, Histidine, Photons, Resonator.

I. INTRODUCTION

A quantum computer is a computation device that makes direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data.[1] Quantum computers are different from digital computers based on transistors. Whereas digital computers require data to be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses qubits (quantum bits), which can be in superposition's of states. A theoretical model is the quantum Turing machine, also known as the universal quantum computer. Quantum computers share theoretical similarities with non-deterministic and probabilistic computers; one example is the ability to be in more than one state simultaneously.

II. BASIS FOR QUANTUM COMPUTING

A classical computer has a memory made up of bits, where each bit represents either a one or a zero. A quantum computer maintains a sequence of qubits. A single qubit can represent a one, a zero, or any quantum superpositionof these two qubit states; moreover, a pair of qubits can be in any quantum superposition of 4 states, and three qubits in any superposition of 8. In general, a quantum computer with qubits can be in an arbitrary superposition of up to different states simultaneously (this compares to a normal computer that can only be in one of these states at any one time). A quantum computer operates by setting the qubits in a controlled initial state that represents the problem at hand and by manipulating those qubits with a fixed sequence of quantum logic gates. The sequence of gates to be applied is called a quantum algorithm. The calculation ends with a measurement, collapsing the system of qubits into one of the pure states, where each qubit is purely zero or one. The outcome can therefore be at most classical bits of information. Quantum algorithms are often non-deterministic, in that they provide the correct solution only with a certain known probability.

III. ISSUES IN QUANTUM COMPUTING

Current approaches to quantum computation exploit the phenomena of entanglement and superposition to create a paradigm that is more powerful than that of classical computing. The field has grown from the exotic arena

confined to a few theoretical physicists into a full scale theoretical and experimental research area with millions of dollars being spent to build prototypes of quantum computers. Many believe that these computers are the only way that one can transcend the eventual limitations of Moore's law, where currently advances have been obtained mainly by advances in lithography. In a quantum computer, the initial state of the quantum register together with the unitary transformations that need to be applied on this state depend of the problem. But this is done mathematically, and it is not clear whether the many hurdles that confront the actual building of these computers will ever be overcome. The main mathematical results related to the exponential speed up provided by the quantum version of the Fourier transform. QUANTUM effects are vital to modern electronics. They can also be a damnable nuisance. Make a transistor too small, for example, and electrons within it can simply vanish from one place and reappear in another because their location is quantumly indeterminate. Currents thus leak away, and signals are degraded. Other people, though, see opportunity instead. Some of the weird things that go on at the quantum scale afford the possibility of doing computing in a new and faster way, and of sending messages that—in theory at least—cannot be intercepted. Several groups of such enthusiasts hope to build quantum computers capable of solving some of the problems which stump today's machines, such as finding prime factors of numbers with hundreds of digits or trawling through large databases. They gave a progress report to the annual meeting of the American Association for the Advancement of Science (AAAS) in Vancouver. At the core of their efforts lie the quantum-mechanical phenomena of superposition and entanglement. An ordinary digital computer manipulates information in the form of bits, which take the value of either 0 or 1. These are represented within the computer as different voltages of electric current, itself the result of the electron's charge. This charge is a fixed feature of all electrons; each has the same amount of it as any other. But electrons possess other, less rigid properties like spin, which can be either "up", "down" or a fuzzy, imprecisely defined combination of the two. Such combinations, known as superpositions, can be used to construct a quantum analogue of the traditional bit—the qubit. Entanglement, meanwhile, is the roping together of particles in order to add more qubits. Each extra qubit in a quantum machine doubles the number of simultaneous operations it can perform. It is this which gives quantum computing its power. Two entangled qubits permit four operations; three permit eight; and so on. A 300-qubit computer could perform more concurrent operations than there are atoms in the visible universe.

IV. A COHERENT IDEA

Unfortunately, such a machine is not in the offing. Entanglement and superposition are delicate things. Even the slightest disturbance causes qubits to "decohere", shedding their magical properties. To build a working quantum computer, qubits will have to become more resilient, and progress so far has been slow. The first quantum computations were done in the lab in 1995. Since then various teams have managed to entangle as many as 14 qubits. The record holders, a group in Innsbruck, use a device called an ion trap in which each qubit exists as a superposition of a rubidium atom at different energies. Raymond Laflamme and his colleagues at the University of Waterloo, in Canada, have managed to entangle 12 qubits by performing a similar trick, entangling certain atoms within a single molecule of an amino acid called histidine, the properties of which make it particularly suited to such experiments. The problem with these approaches is that they will not be easy to scale up. Ion traps reside inside big vacuum chambers, which cannot easily be shrunk. And a molecule of histidine contains only so many suitable atoms. So the search is on for more practical qubits. One promising approach is to etch qubits in semiconductors. Charles Marcus, previously of Harvard University and now at the University of Copenhagen,

has been using electrons' spins to do this. Single-electron qubits decohere quickly, so his team decided instead to create a qubit out of two electrons, which they trapped in "quantum dots", tiny semiconducting crystals (of gallium arsenide, in this case). When two such dots are close together, it is possible to get an electron trapped in one to pop over and join its neighbour in the other. The superposition of the two electrons' spins produces the qubit. Dr Marcus's team have so far managed to stitch four such qubits together. An array of clever tricks has extended their life to about ten microseconds—enough to perform the simple algebraic operations that are the lifeblood of computing. They hope to extend their life further by using silicon or carbon, the atomic nuclei of which interfere less with the entangled electrons than do those of gallium arsenide. John Martinis and his colleagues at the University of California, Santa Barbara (UCSB), meanwhile, have been trying to forge qubits from superconducting circuits. In a superconductor, electrons do not travel solo. Instead, for complicated quantum-mechanical reasons, they pair up (for the same reasons, the pairs feel no electrical resistance). When they do so, the pairs start behaving like a single particle, superposing proclivities and all. This superparticle can, for instance, in effect be moving in two directions at once. As electrons move, they create a magnetic field. Make a closed loop of superconducting wire, then, and you get a magnetic field which can be facing up and down at the same time. You have yourself a superconducting qubit—or five, the number Dr Martinis has so far managed to entangle. He has another clever trick up his sleeve. Using a device called a resonator he has been able to transfer information from the circuit to a single photon and trap it in a cavity for a few microseconds. He has, in other words, created a quantum memory. A few microseconds may not sound much, but it is just about enough to perform some basic operations. The problem with all these approaches is that the quantum states they rely on are fragile, which allows errors to creep in. One way to ensure that they do not scupper the calculation is to encode the same information in several qubits instead of just one. Drs Marcus, Martinis and Laflamme have therefore had to build redundant qubits into their systems. For every "logical" qubit needed to do a calculation, there is a handful of physical ones, all of which need to be entangled. Michael Freedman is trying to address this problem by taking a different tack. Together with his colleagues at Microsoft's Station Q research centre, also at UCSB, he is trying to build what he calls a topological quantum computer. This uses a superconductor on top of a layer of an exotic material called indium antimony. When a voltage is applied to this sandwich, the whole lot becomes a quantum system capable of existing in superposed states.

V. WHAT QUANTUM COMPUTERS CAN DO FOR US

To begin with, there are still many issues that must be solved before a practical, working quantum computer can be achieved. A quantum computer is not something that we can expect to be using any day soon. The completion of a quantum computer, however, will make it possible to instantly solve problems that require exhaustive calculations by "brute force," a method that existing computers are not particularly strong at. Problems of this type include the computing of prime factors and the solving of NP-complete problems that must consider the combination of a vast number of events. We can also expect the quantum computer to be applied to quantum simulations for analyzing complex quantum systems such as protein reactions and catalytic material, and to secure communications based on quantum cryptography. At the same time, it is sometimes mistakenly thought that any type of computation will be accelerated by a quantum computer. This misunderstanding originates with the false idea that a quantum computer achieves high speed in the same way that a personal computer would by increasing the speed of its CPU. Let's take the case of calculating 1+1 in a quantum computer. The time required for performing this simple calculation and outputting its result would not be very different from that of an

existing computer. In short, the wonderful features of the quantum computer will probably not be appreciated as long as we think of it in terms of the computers that we now use in our daily lives. However, for specialists that are working on problems adequate for the quantum computer and that wish to perform computations that would require a huge amount of time even for a supercomputer, the quantum computer is a dream come true. The following graph shows how existing computers and quantum computers are expected to evolve in terms of integration and information-processing capacity. According to Moore' Law, which states that data density in semiconductor devices doubles every 18 months (an empirical law first observed by Gordon Moore in 1965), the length of high-speed semiconductor gate electrodes in existing computers should reach 6 nm by the year 2020. Concerning this area of research, NEC announced the successful development of a 5-nm transistor in December 2003. A transistor size of 5 nm, however, is thought to be the limit of device miniaturization in terms of operating principles. The quantum computer, on the other hand, will eventually surpass the information-processing capacity of existing computers as the number of quantum bits steadily increases.

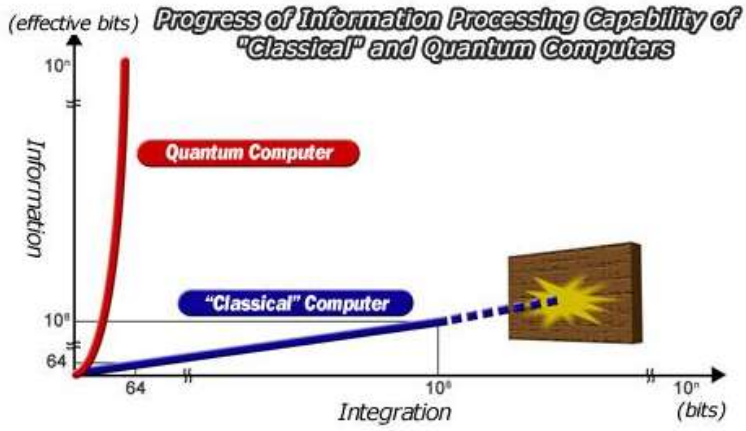

Fig.1 Progress Of Information Processing Capability Of "Classical" And Quantum Computers

VI. WHAT WILL QUANTUM COMPUTERS BE USED FOR IN THE FUTURE

Like any technology that hasn't quite passed from science fiction to science fact, quantum computers have had high expectations placed on them. But with the arguably slow process in the development of quantum computers, as well as the discovery that their uses may be more limited than initially theorized, these heavily hyped machines have fallen somewhat in prestige. Even MIT's news service saw fit to publish a headline in 2009 that read, "Quantum computing may actually be in useful". In truth, quantum computers may have wide applications, but it's difficult at this relatively early stage to do anything more than guess what those might be. We know that quantum computers will be better than traditional computers at decryption, owing to their ability to quickly factor large numbers. That MIT news article pointed to a study that found that quantum computers would be useful for solving systems of linear equations, making them useful for highly complex calculations -- like modeling proteins or weather systems. Quantum computers could also make searches much more efficient, which have drawn the attention of the world's largest Internet companies. In December 2009, Google published a post on one of its blogs about the company's research into using quantum computers for image search. Google's efforts have found that quantum computers can search for a particular image, or recognize an object within a larger image (in this case, a car), much faster than a traditional computer . But some critics have questioned whether the machines provided by D-Wave Systems, the company working with Google on the project, even

qualify as quantum computers. D-Wave uses some novel methods to produce its computers (it's not clear if the company makes proper use of "entanglement," a phenomenon essential to quantum computing), and some scientists have said that its claims of producing 128-qubit computers don't seem credible. (A qubit is a unit of quantum information that can be 0, 1 or 0 and 1 simultaneously.) In research settings, most quantum computers have topped out at far lower levels, such as 4 or 8 qubits. Even as some experts question its claims, D-Wave has achieved mainstream recognition, publishing papers in the journal "Nature" and selling one of its 128-qubit machines to Lockheed-Martin -- the first commercial sale of a quantum computer.

VII. THE FUTURE OF QUANTUM IT

The word "quantum" can conjure images of scientists working on technology that will one day allow time travel, or, at the very least, permit travel to alternate realities. Although such developments may currently be confined to an episode of Dr. Who, the use of quantum information technology in business computing will become a reality within the next ten years, says Andrew Shields, leader of the quantum information group at Toshiba's Cambridge Research lab. Shields and his team have made a breakthrough that they say will allow information to be captured and returned to the user in a meaningful form after having been processed by a quantum IT program. Shields says this would allow future computers to process complex computations in four months. This may seem like a long time, but it would take a 1Ghz computer of today's standards longer than the age of the universe to perform the same calculations.In traditional computing, a bit is a fundamental unit of information, represented in binary as 0 or 1 and stored as an "on" or "off" signal on an electronic circuit. If you search a database for a particular result, the computer program methodically analyses each row of data in the database, bit by bit, for a positive match. Where there is a match, the database returns a value of "true" (where true is the binary state "1") or "false" (binary state "0") for no match.In a quantum computer, the fundamental unit of information is a qubit. Qubits are stored on particles of light called photons. A qubit can exist not only in a state corresponding to the logical values 0 or 1, but also in states corresponding to a blend or superposition of these values. When searching a database in quantum computing, the program would be able to "see" all results at once from a superposition instantly, rather than having to move through each row. "The net effect of quantum computing is that data can be processed much quicker than under a traditional computing model," says Shields. The other benefit of quantum computing is that it can enable secure communications over optical fibre links. This is where scientists at Toshiba labs believe they have made progress. They say they have developed the first practical semiconductor device that can count the particles or photons in light signals. The new device is a significant step towards viable quantum computers and communication systems, which exploit the particle-like properties of light. Counting photons is necessary when sending secret digital keys over long distances. "A simple semiconductor device that can count the photons in a light signal is important for several quantum applications. You can prevent eavesdropping on optical fibre links by counting if the photons have been interfered with," says Shields. Lack of a suitable photon number resolving detector has been a major obstacle to real-world deployment of quantum technologies, says Shields. In principle, quantum key distribution provides a secure means for transmitting secret keys between two parties on fibre optical networks. However, the QKD systems developed so far are vulnerable to hacking. The weak laser diode used to generate single photon pulses that carry the quantum keys, will sometimes generate pulses with multiple photons. As a result, an eavesdropper could split off one of these extra photons and measure it, while leaving the other photons in the pulse undisturbed, thus determining part of the key while remaining undetected. Furthermore, an eavesdropper can determine the entire key, by blocking the

single-photon pulses and allowing only the multi-photon pulses to travel through the fibre. "Using these new methods for QKD we can distribute more secret keys per second, while at the same time guaranteeing their unconditional security. This enables QKD to be used for a number of important applications such as encryption of high bandwidth data links," says Shields.Until now the most common semiconductor detector, the avalanche photo-diode, has been able to register only the presence or absence of one or more photons. The detector, developed by Toshiba, however, is able to count the number of individual photons in a pulse. It is the first practical device with this capability. The breakthrough is a result of a new technique developed by Toshiba to detect weak photon-induced avalanches. The electrical current caused by a single photon in a semiconductor is too weak to be detected quickly. Avalanche photo-diodes work by amplifying this current a million-fold using an avalanche effect. Usually, however, the strength of the final current does not depend on the number of photons that initiated it. The Toshiba device can detect photon-induced avalanches 20 times weaker than conventionally, and the strength of which scale with the incident number of photons. It is a step in the right direction for quantum computing but there are many challenges that must be overcome before quantum computing becomes mainstream. "We need lots of new technology for quantum computing to take off, such as quantum memory," says Shields.Quantum memory can store information in quantum states. However, this is something the industry does not currently have. Quantum logic gates and sensors that can accurately detect quantum states are also pre-requisites. Nevertheless, Shields remains confident that with the developments of his lab, it will be only a matter of time before we are all taking a quantum leap forward in computing.

VIII. CONCLUSION

After carrying out a review onto quantum computing technology and its future aspects we conclude that Quantum Computation relies on quantum mechanics which is a mathematical model that describes the evolution of physical realization of computation and hence the computer itself. It definitely provides a promising base which may provide solution to the upcoming challenges in the field of computational science.

REFERENCES

[1] R. Landauer, Irreversibility and heat generation in the computing process.IBM J. Res. Dev. 5: 183-190, 1961.
[2] 2.H. D. Zeh, On the interpretation of measurement in quantum theory. Found. Phys. 1: 69, 1970.
[3] J. D. Bekenstein, Black holes and entropy. Phys. Rev. D 7: 2333-2346, 1973.
[4] 4.S. Kak, On quantum numbers and uncertainty. Nuovo Cimento, 34B: 530-534, 1976.
[5] 5.C.H. Bennett, The thermodynamics of computation – a review. Int. J. Theo. Phys., 21, pp. 905-940, 1982.