The Concept and Future of Quantum Computing

Niramay Sanghvi
Student, Dept of EXTC
D. J. Sanghvi College of Engineering
Mumbai

Varun Varadan
Student, Dept of EXTC
D. J. Sanghvi College of Engineering
Mumbai

Avi Shah
Student, Dept of EXTC
D. J. Sanghvi College of Engineering
Mumbai

Aman Shah
Student, Dept of EXTC
D. J. Sanghvi College of Engineering
Mumbai

ABSTRACT
Quantum computing is a new and emerging field which shows great promise. It abandons the traditional approach of using transistors to store and update logical data, instead using subatomic particles(most often electrons) for the same purpose. The aim is to introduce the topic of quantum computing in a manner which would prove understandable to the reader by eliminating unnecessary jargon. The necessity of using quantum computing in order to keeping up with current advancements and the needs of new computing systems will be made apparent.

The field of quantum computing is relatively new and much of the research and effort going into developing it is nascent. If the potential can be harnessed, however, the prospects of using quantum computers to solve problems which cannot be solved using their traditional counterparts hold great promise.

Keywords
CTD Principle, Quantum Superposition, Quantum Entanglement, Qubits, Bloch sphere.

1. INTRODUCTION
Classical computing requires the usage of bits, i.e. a set of values that can be either 'high'(1) or 'low'(0) depending upon the value assigned to them, to store information.

Instead of using classical bits to store its information, quantum computing allows us to harness the potential of quantum bits, or 'qubits' as they're commonly called. Qubits differ from classical bits in that they can be in varying states at the same time, owing to the phenomena of quantum superposition and entanglement. Hence, they need not be confined to a set of 'high' and 'low' values, as they can occupy a variety of states other than them.

The potential for improvement of computers remains enormous. Due to the ability to store a vast number of values other than the logical high and low values means that it can greatly increase the computational power of computers. And the increase of computing power is necessary to satisfy our need for better computers. Classical computing can only satisfy the predictions set forth by Moore's law till a certain time in the future, after which one would have to resort to other means of increase computing capacity, one of which includes the usage of quantum computers.

While one may not be able to use quantum computing for all processes currently handled by conventional computers, one can use it for other purposes, such as to increase our knowledge and understanding of how quantum processes work according to the Church–Turing–Deutsch principle(CTD Principle).

2. MOORE'S LAW AND CLASSICAL COMPUTERS
In order to understand why research in the field of quantum computing is gaining importance, one has to understand Moore's law and the limitations suffered by classical computers in keeping up with the law. [1]

Gordon Moore, co-founder of the Intel Corporation, stated in a 1965 paper that the amount of transistors that could be incorporated into an Integrated Circuit(IC) would double approximately every two years. This law showed reasonable accuracy in predicting the growth in computing for around 40 years. An example to show the accuracy of this law would be the fact that the number of transistors per IC in 2006 was around 300 million, which was reasonably accurate as compared to the figure of 301.456 million predicted by Moore's law, if one considers the number of transistors in 1972(2300) as the benchmark for predictions.

This increase in the number of transistors can be regarded as being beneficial, as it leads to an exponential increase in computational ability and efficiency.

However, in the last 8 years, the number of transistors used in classical computers has not kept up with these figures. While the transistor count predicted by Moore's law in 2014 is approximately 4.823 billion (taking into account the previous benchmark), the actual transistor count has reached a maximum of only around 1.5 billion. It is clear that scientists have reached a limit as far as the exponential growth predicted by Moore's law is concerned. [2]

The problem lies in the fact that increasing the transistor count would involve reducing the size of transistors in order to increase their density on an IC. There is only a certain limit till which one can reduce the size. The usage of transistors relies on their effective functioning as a switch between an 'on' and an 'off' state. When the transistor—generally an Enhancement mode MOSFET (E-MOSFET)—switches off, it leaves behind a certain non-conducting gap between two conducting regions through which electrons must not flow. With the current developments in transistor sizes, this gap is only 32 nanometres across, i.e. a few hundred atoms of silicon, the material out of which most transistors are made. If one further reduces this gap, reaching lengths of around 14 nanometres, electrons flow across it nonetheless, through the process of quantum tunnelling. This results in the corruption of data.

Other difficulties involved with sizes in the order of nanometres and high transistor counts include unreliability of chips due to the fact that a mistake in fabrication of only a few atoms would render the chip useless, as well as the large amount of power dissipated in the form of heat.

3. EARLY RESEARCH AND DEVELOPMENT

As mentioned earlier, quantum computing is a relatively new field, with seminal research only taking place after 1970.

In the 1970s and early 1980s, physicists and computer scientists made predictions based on Moore's law to determine the limitations of classical computers, and they realized that an alternative for classical computers had to be found. Richard Feynman, a prestigious scientist who was famous for his research on various topics related to quantum mechanics, discussed the possibility of using quantum systems for computational purposes. Furthermore, he hypothesized that a quantum computer could also be used to carry out experiments on quantum mechanical processes.

In 1985, David Deutsch built upon Feynman's hypothesis, stating that any finitely realizable physical process could be simulated by using a quantum computer. His contributions shall be discussed under the section of this paper concerning the CTD principle.

In 1994, Peter Shor developed an algorithm which proved that quantum computers could factorize large numbers in a fraction of the time taken by conventional computers to do the same. [3]

4. QUBITS

Quantum computing has been suggested as a way of solving the aforementioned problems that are faced by traditional computers, as it does not involve the usage of transistors. In quantum computing, the unit of information storage is termed as a quantum bit, or a 'qubit.' Generally, an electron is chosen as a qubit, e.g. the outermost electron of a phosphorus or silicon atom, although photons and nuclei can be used as qubits also.

Quantum systems utilize two important phenomena: quantum superposition and quantum entanglement.

4.1 The Bloch Sphere

The principle of quantum superposition regarding qubits can visualized by using the bloch sphere, [4] as shown below:

Quantum superposition is a property displayed by a particle that exists in a variety of possible states, such that only one out of the large number of possibilities can actually be observed at a particular instant. In quantum computing, superposition manifests itself in the way that electrons can exist between the two extremes of being in two basis states, e.g. the 'spin-up' and spin-down state of an electron.

There are two basis states of the qubit under consideration can be represented as |0> and |1>. The qubit can be thought of as a linear combination of these two states, i.e. a superposition of the two basis state, as:

$$|¥> = \alpha|0> + \beta|1>$$

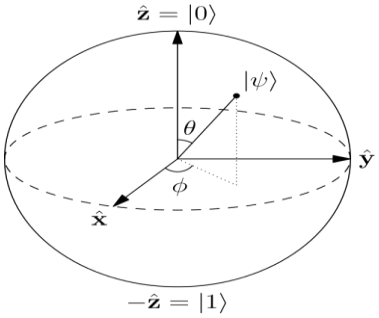

Fig 1: The Bloch Sphere

α and β are the probability amplitudes of the two states. The probability of each state is given by $|\boldsymbol{\alpha}|^2$ and $|\boldsymbol{\beta}|^2$. The state must be normalized, i.e. $|\boldsymbol{\alpha}|^2 + |\boldsymbol{\beta}|^2 = \mathbf{1}$, as the sum of probabilities of both states is 1.

Hence, the choice of probability amplitudes is given by $\boldsymbol{\alpha}=\cos\boldsymbol{\theta/2}$ and $\boldsymbol{\beta} = \boldsymbol{e^{i\emptyset}}\ \sin\boldsymbol{\theta/2}$. The surface of the bloch sphere represents the pure states of existence of the qubit, and they are an adequate representation for when the qubit is isolated.

However, when the qubit is coupled with other quantum mechanical objects, it might exist in a mixed state, i.e. a combination of pure states, with the points inside the sphere representing the mixed states.

5. STORAGE USING QUBIT REGISTERS

If more than one qubit must be used, i.e. qubit registers, to store information, then one has to consider the effects of quantum entanglement. Qubit registers are important, since they allow us to design quantum logic gates. [5]

Quantum entanglement is the phenomenon via which a variety of quantum mechanical particles interact with each other, such that the state of any one particle cannot be considered separately. In such cases, the behaviour of the entangled system of quantum particles must be considered.

Considering two qubits, one of the possible states would be as follows:

$$|¥> = 1/\sqrt{2}(|00> + |11>)$$

The states of both electrons must be considered as a whole, in accordance to the principle of quantum entanglement. There are $2^2 = 4$ possible states which can be defined thusly. Corresponding to each state, one can attach four different coefficients α, β, γ and δ. If use N qubits are used, there are 2^N different states involved, with 2^N different coefficients that can be attached to each state. The summation of the product of each state and the corresponding coefficient gives us the total state of the entangled system. Each coefficient represents a distinct value of information that can be obtained from the system. Hence, by using a system of N qubits, i.e. a **qubit register**, one can contain the same amount of information that is stored using a register of 2^N classical bits. It can thus be observed that the storage capacity increases exponentially with the usage of quantum computers.

6. READING AND WRITING INFORMATION

Breakthroughs in reading and writing information using qubits were made by Australian engineers at the University of New South Wales, who created the first working qubit in 2012. The experimental setup used by them can be described as follows:

The qubit used is a single electron of a phosphorus atom, which was implanted next to a silicon transistor, an E-MOSFET. [6] The basis states used for measurement are the spin states of an electron, i.e. whether the electron is in 'spin-up' or a 'spin-down' state. The entire setup is cooled down to a temperature close to absolute zero in order to avoid any unnecessary oscillations between the two basis states due to thermal energy.

Under such conditions, an electron exists in the 'spin-down' state, which has lower energy. However, one can increase the energy to make the electron enter the 'spin-up' state, by irradiating it with microwave energy of a certain frequency. The frequency of the microwave radiation depends upon the external magnetic field surrounding the electron, which is controlled via a superconducting magnet. Hence values can be 'written' to the qubit to change its state.

When the electron reaches the 'spin-up' state, it transfers to the gap between the drain and source terminals of the E-MOSFET. As a result, the gap conducts electricity when it a voltage is applied across it, which manifests itself as a spike in current. If the electron was in a 'spin-down' state, then no conduction would have occurred, as the electron would have lacked the energy to transfer itself to the gap. By observing the spikes in current, one can ascertain whether the electron was in a 'spin-up' or a 'spin-down' state, and hence one can 'read' the value stored in the qubit.

7. APPLICATIONS OF QUANTUM COMPUTERS

The field of quantum computing has opened many new avenues to solve problems previously thought of as unsolvable. A few of them are mentioned in this section.

7.1 Factorization and Cryptanalysis

Quantum computing has applications in the field of cryptanalysis.[7] As mentioned earlier, Peter Shor developed an algorithm, called the Shor's algorithm for the factorization of large numbers in a small amount of time.

His research sparked an interest in the usage of quantum computers for cryptanalysis and breaking cryptosystems; the difficulty in the factorization of large numbers is the foundation of many encryption algorithms such as the RSA algorithm and other public key encryption algorithms, which use the product of two large prime numbers. Trying to factorize and break a 2048 bit encryption key made by Digicert, a common SSL provider, can take a desktop computer approximately 6.4 quadrillion years. However, the factorization of 2048 bit numbers can be achieved in mere minutes by using a quantum computer. This is due to the fact that quantum computing greatly reduces the number of steps involved in the factorization.

The efficiency of Shor's algorithm is largely due to the efficiency of the quantum Fourier transform. The time taken by Shor's algorithm to factor a very large integer N tends to a polynomial function of $\log N$ as N approaches infinity. As logarithmic values of large are much lesser than the numbers themselves, this indicates that the time taken to factorize large numbers by using quantum computers is greatly reduced, especially in comparison to classical computers.

Other algorithms for the factorization of large products of prime numbers using quantum computation have also been developed. In November 2011, physicists at the University of Science and Technology of China in Hefei, China factorized the number 143 using a quantum computing algorithm using Adiabatic Quantum Computation. [8] This remains the largest number to be factorized using quantum computation.

7.2 The CTD Principle and the Realization of a Universal Turing Machine Using a Quantum Computer

In 1936, Alonzo Church and his student, mathematician Alan Turing, hypothesized that every naturally computable function and every physical process could be simulated by the universal Turing machine. Hence, a function can be considered to be naturally computable if and only if it can be computed by a Turing machine.

However, in 1985, David Deutsch recognized the limitations of the Church-Turing thesis, as it would come to be known. [9] The Church-Turing thesis cannot be applied to classical physical processes. To understand why, let us consider a computing machine M which can compute a set of functions given by C(M). C(M) is said to be computationally equivalent to a physical process if it can give the same output as the physical process under the same input. However, the set of realizable functions C(M) is always contained within C(T), which represents the set of computable functions for a universal Turing machine. Since C(T) is countable, the output given by the universal Turing machine will always be infinitely lesser than all the possible values for processes in classical physics, which are continuous in nature and hence have an infinite number of possible outputs.

Hence, Deutsch in his 1985 paper, *Quantum theory, the Church-Turing principle and the universal quantum computer*, stated a modification of the earlier Church-Turing thesis, taking into account the finite nature of computational systems.

'Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means'

In addition to having stated this principle, David Deutsche went further, discussing the prospect of a universal computing device and the suitability of quantum computers as universal computing devices. He proved that a quantum machine could simulate all zero temperature systems with a very high (but not 100%) accuracy, including other quantum computers and various quantum mechanical processes.

7.3 Keeping up with Moore's law

As discussed earlier, quantum computers are now being used to surpass the limitations suffered by earlier, classical computers due to effects such as quantum tunnelling and heating. They might be able to continue the trend predicted by Moore's law, which classical computers have not been able to do of late.

8. LIMITATIONS OF QUANTUM COMPUTING

It is important to note that the field of quantum computing is still in its infancy. [10] Many limitations associated with it have been found in various experiments, some of which are as follows:

8.1 Quantum Decoherence

Quantum decoherence is the loss of ordering between phase angles, often due to the interference of the quantum system under observation with outside influences. [11] The very fact that quantum computers need to be isolated from outside systems to work properly poses a problem, as true isolation is very difficult to achieve. Even a stray magnetic field can greatly affect the output of a quantum computer.

8.2 Obtaining a Valid Output

An important limitation of quantum computers lies in obtaining a measured output value that corresponds to one of the basis states of the qubits. Designing the logical operations needed to achieve this is challenging, as a quantum system can be in a vast number of superpositions of different states at a particular instant. Not all of these can be measured; only the outputs corresponding to the basis states are measurable.

A large number of computations might have to be performed using a quantum computer before a correct output is obtained, hence reducing the speed of the process. The fact that even observing a qubit might change its state further compounds the problem.

9. CONCLUSION

In summary it can be said that, despite suffering from limitations, quantum computation holds vast potential. David Deutsch proved that quantum computers could be used to simulate any quantum system, aiding research in the field of quantum mechanics. Peter Shor predicted the usage of quantum computers to solve problems in cryptanalysis and factorization much faster than classical computers. The first working qubits have already been created, using both electrons and nuclei.

Due to the disadvantages of quantum computers, they cannot be used to replace classical computers altogether. Instead, the use of quantum computers lies in occupying new niches previously unoccupied by their classical counterparts, such as making a universal computing machine or the factorization of large numbers. Thus, the true potential of quantum computers lies in addition, not replacement.

10. REFERENCES

[1] Schaller, Robert R. "Moore's law: past, present and future." Spectrum, IEEE 34.6 (1997): 52-59.

[2] Aaronson, Scott, and Dave Bacon. "Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment." Computing Community Consortium, and Version 6 (2008).

[3] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM journal on computing 26.5 (1997): 1484-1509.

[4] Glendinning, Ian. "The bloch sphere." QIA Meeting. Vienna. 2005.

[5] Monroe, Chris, et al. "Demonstration of a fundamental quantum logic gate." Physical Review Letters 75.25 (1995): 4714.

[6] O'Brien, J. L., et al. "Towards the fabrication of phosphorus qubits for a silicon quantum computer." Physical Review B 64.16 (2001): 161401.

[7] Brassard, Gilles, Peter Høyer, and Alain Tapp. "Quantum cryptanalysis of hash and claw-free functions." LATIN'98: Theoretical Informatics. Springer Berlin Heidelberg, 1998. 163-169.

[8] Xu, Nanyang, et al. "Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system." Physical review letters 108.13 (2012): 130501.

[9] Deutsch, David. "Quantum theory, the Church-Turing principle and the universal quantum computer." Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 400.1818 (1985): 97-117.

[10] Aaronson, Scott. "The limits of quantum computers." Scientific American 298.3 (2008): 62-69.

[11] Bittner, Eric R., and Peter J. Rossky. "Quantum decoherence in mixed quantum-classical systems: Nonadiabatic processes." The Journal of chemical physics 103.18 (1995): 8130-8143.