Quantum Computation: An Overview

Adithya Narayan[*1], Aravind Harinarayanan[*2], Sonus Vareed[*3]

[*1 2 3] *School of Computer Science and Engineering (SCOPE), VIT Vellore, Tamil Nadu, India*

---***---

ABSTRACT

Quantum theory is one of the most advanced and progressive fields of science today. It has given way to new horizons in modern technology. It has also opened the possibility of expressing and communicating information in different ways. Up until now the information was always expressed and communicated through physical or digital ways. In this paper we provide an in-depth look into the major concerns of Quantum computing and Quantum machine learning.

Keywords: Quantum Computing, Quantum Machine Learning, Qubits, Computer Evolution

I. INTRODUCTION

Ever since the introduction of the basic Computer in 1837 by Charles Babbage computers have undergone extraordinary development from its 30-ton ancestor to the high-speed modern Computer, we see today. Even though computers have undergone vast changes in these years, it is important to note that its fundamental principle remains the same, i.e., to interpret and manipulate an encoding of binary digits into a useful computational result.

The number of atoms required to represent a bit of memory has decreased exponentially as computers evolved from the early valves, gears and vacuum tubes to the integrated chips and microprocessors we see today. This is the basis of the Moore's Law, which states that computer processing power doubles every eighteen months.

Now if we extrapolate the graph of Moore's Law, we can infer that sooner or later each bit of memory should be encoded by particles of subatomic size.

This point is also supported by the survey made by Keyes in 1988 as shown in figure below.

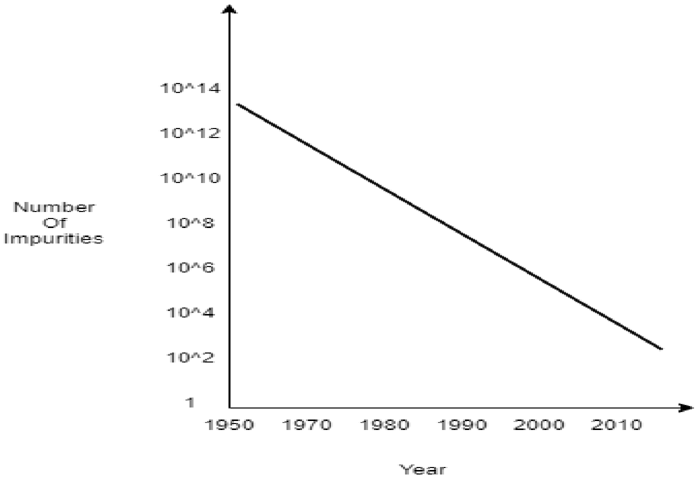


Fig:1. Showing the number of dopant impurities in a bipolar transistor logic with year.

1. This is a plot which shows the number of electrons required to store a single bit of information.

2. By extrapolating this plot, we can infer that we might be within the reach of an atomic scale of computations within a decade.

3. An analysis of the plot suggests that we might be within the reach of atomic scale computations within a decade or so at the atomic scale however.

Subatomic particles are governed by quantum mechanics which are quite different from the classical logic, which determine the properties of conventional logic gates.

So, by Moore's law if computers are to become smaller in future, new, quantum technology must replace the conventional classical technology. Quantum technology can not only decrease the size and multiply the clock seed of microprocessors but it can also support new algorithms which are quantitatively and qualitatively better.

With the size of the components shrinking into subatomic sizes, scientists have begun to investigate the potential of quantum behaviors for computation. Astonishingly it seems that a computer which functions in a quantum way is more powerful than any classical computer can ever be. The physical limitations of a classical computer and the possibility of a quantum computer to perform certain useful tasks more quickly than any classical computer drive the study of quantum computing.

Quantum computing opens up new realms in the fields of parallelism and mass computation, it also has a memory which is exponentially larger than its apparent physical size. A few and simple concepts from quantum mechanics are needed to make quantum computers a possibility. If the quantum computer is an inevitability or an impossibility is the million-dollar question.

II. LITERATURE REVIEW

History of Quantum Computing

The idea of using quantum mechanics in computational devices was first explored in the 1970's by Charles H Bennet, Paul Benioff, David Deutsch and Richard P. Feynman. Feynman was among the few who tried to provide the concept of a new kind of Computer which was based on the principles of quantum physics. He also constructed an abstract model which shows how a quantum system could be used to do computational calculations and also predict that it could be used to simulate physical problems which pertained to quantum physics which was impossible until then. That is, he could analyze that this quantum mechanical computer could be used to solve the problems which a classical computer could not, especially those pertaining to quantum mechanical body problems and those which if we had tried to solve on a classical computer would require exponentially growing time.

Later, Deutsch realized that Feynman's assertion could eventually lead to a general-purpose quantum computer. He further proved that any physical process, in principle could be modelled perfectly by a quantum computer. Thus, opening up unlimited possibilities in comparison with a classical computer. Peter Shor In 1994 showed that a quantum computer could be used to factor huge numbers immensely fast. Thus, transforming the field of quantum computing from just an academic curiosity to a sensation the world over.

Potency of Quantum Computing

A quantum computer with 500 qubits (refer appendix) will have 2500 superposition (refer appendix) states, wherein each state is equivalent to a single list of 500 binary digits (1's and 0's) in a classical computer. Theoretically such a computer could operate on 2^{500} states simultaneously. Also, by the laws of quantum mechanics observing such a system will cause it to collapse into a single quantum state, giving a single answer i.e., a single list of 1's and 0's. Hence this kind of Computer is equivalent to 10^{150} processors in a classical computer.

Drawbacks of Classical Computing and Advent of Quantum Computers

In 1970 the concept of public key encryption system was introduced. It was based on the principle of a safe with two keys, one public key to lock it and one private key to open it. Basically, it means that anyone can lock the safe but only one person can open it. In reality these keys are just large integers. It is also easy to derive a public key from a private key but not vice versa. This is because this system is based on the principle that mathematical operations can be done quickly in one direction but not the other. e.g.: multiplication over factorization.

In the case of factorization, the use of computational resources is immense as we keep increasing the number of digits. The public key cryptosystems are based on the assumption that the factorization of large integers is very difficult. Most encryption algorithms today like the RSA, DES are based on the assumption that using the technology today even the fastest computers would take millions of years to crack the encryption. But by quantifying the factorization of large numbers this time can be exponentially reduced

Quantum Factorization vs Classical Factorization

The factoring of big numbers remained beyond the capabilities of any realistic computing devices because up until now no one considered that quantum computation could be employed to perform such operations. According to the algorithm developed by Peter Shor factoring an integer using a quantum computer runs in $O((\ln N)^{2+\epsilon})$ steps where ϵ is very small compared to O(exp((64/9)1/3(lnN)1/3(ln lnN)2/3)) of a classical computer.

That is, factorizing a 1000-digit number will require only a few million steps for a quantum computer compared to which a classical factorization system which would take more than 12 billion years to factorize a 100-digit number. This, suggests the futility of public key-based cryptosystems.

Other major problems that a quantum computer has a great advantage over a classical computer are:

1. Searching of an item with a specific property from a collection of N items.

2. Simulation of a quantum system: By using a quantum computer we can solve the problem of polynomial slowdown which generally occurs in a classical computer.

Quantum Computing and Parallelism

Parallelism is a concept in computation which refers to running multiple calculations or multiple processes simultaneously. Classical computers are inherently inefficient to carry out parallelism. This, is because in classical computers the microprocessors operate such that the primary test is first divided into smaller or fundamental tasks and these tasks are carried out serially one at a time. The progress of classical Computer in parallelism has been very slow and unsteady. This is mainly due to the fact that in classical computers the CPU is rapidly cycling from one task to the other thus creating the impression that it is running multiple tasks simultaneously. Hence this is not true parallelism. This can only be achieved by using a quantum computer, i.e., by implementing quantum parallelism. We can understand the quantum state as a superposition of many classical and classical like states. If this superposition can be protected from entanglement with its environment (decoherence) a parallelism can be set up on a serial machinelike quantum parallelism.

Other Benefits of Quantum Computing

Artificial intelligence: Being much faster and able to do more calculations at a very short amount of time, quantum computers could learn faster even by using the simplest mistake bound model (refer appendix). It will also aid us in developing complex compression algorithms, voice and image recognition, molecular simulations, true randomness and quantum communication. It can also make communication become more secure because with the help of quantum communication both receiver and sender are alerted when a third party tries to catch the signal. It can also increase the speed of communication by allowing more information to be communicated per bit.

Quantum Entanglement and Decoherence

By the basic principle of quantum mechanics that when no external system is interacting with our original system then our system will be a blend or superposition(ref)of all four quantum states. It also states that if we try to measure any of the features of this system then we cause the system to collapse into any one of the states. If something interacts with one part of our system the whole system will be affected. i.e., we can judge or calculate the spin of one particle by just determining the spin of the other entangled particle. This is the basis of quantum computing; it essentially means that to get the information in 2^N bits we would only require N qubits or N qubits can contain the information in 2^N bits. The qubits in quantum computer can exist in multiple states at the same time. i.e., it can be 0 and 1 at the same time. And by the principle of quantum entanglement to determine the value of 4 qubits we only need to the values of 2 qubits. Hence drastically effecting the speed and functioning of the processor.

Drawbacks of quantum systems

Decoherence

It refers to the loss of quantum coherence. Quantum particles act as waves and can be defined by using wave functions as long as there is a phase relationship between different states it is said to be coherent. This coherence is the basic property of quantum mechanics and is an essential part of quantum computing. However, when a quantum system is not totally isolated but is in contact with its surroundings it loses its coherence over time. This process is referred to as quantum decoherence. As a result of this process the quantum behavior is lost. It can lead to the loss of information.

Cost of Production

The cost of production of a quantum computer is also a major milestone. In 1997 Gerstenfeld and Chuang made the first quantum computer based on magnetic resonance technology. It was just a simple searching program using Grover's algorithm. The price of making this 2 – qubit computer was approximately $1 million.

Other Major Requirements

Scientists, engineers and physicists who are trying to execute quantum operations face two major problems:

1. The qubits need to be shielded from the external environment, otherwise it could destroy the delicate quantum states required for computation. Moreover, longer we can maintain a qubit in its desired state greater will be the coherence time and hence more efficient the computation.

2. For the execution of the algorithm the qubits have to be entangled and also controllable on demand. Hence the perfect balance between isolation and interaction is crucial.

Quantum Interference and Quantum Superposition - Theoretical visualization of quantum computer

Just like the fundamental unit of light is known as photon, in a quantum computer the fundamental unit of information is called a "qubit". The qubit is analogous to the bit which is the fundamental unit of ordinary computers, but unlike the bit which is binary qubit is more quaternary in nature. This unique property of a qubit is actually a consequence of its adherence to follow the laws of quantum motions. A bit can exist as 1 or 0 (classical states) however a qubit exists not only as 1 and 0 but also in states that are a blend of superposition of the given classical states. In simple words a qubit can exist as 0,1 or simultaneously as both 0 and 1, along with a coefficient that represents the probability of each state. Such a concept is different from the laws of classical physics and obeys laws of quantum mechanics which become significant at the atomic level. A qubit can be visualized having a spin of half of an electron system, the two states being the +/- of the basic spin that is + 1/2, - 1/2. These two states indeed represent the two Eigenstates (refer appendix) of the z component of an external magnetic field of same magnitude of spin. The existence of qubit seems strange but in reality, a beam of single photon can be used to represent a qubit. The different states will be the states of polarization (horizontal or vertical) with respect to a chosen axis. Thus, the qubit takes 0,1 as the value which are then associated with two eigenstates of a spin of an electron.

$$|1> = |\uparrow>$$
$$|0> = |\downarrow>$$
$$|0> + |1> = |\uparrow> + |\downarrow>$$

Qubit can exist not only in these states but also in states that are a superposition of the given states which have complex coefficients and this property distinguishes a qubit from the normal bit. A state of a qubit can be described by the given equation:

$$\alpha|0\rangle + \beta|1\rangle$$

Here α, β are complex number which satisfy the equation:

$$|\alpha|^2 + |\beta|^2 = 1$$

In mathematical terms since the general state of a qubit is the superposition of two pure states with complex coefficients, the state is described as a vector in the complex two-dimensional space and the pure states form the basis of this representation. One of the most famous experiments that demonstrate quantum superposition is the beam splitting of light.

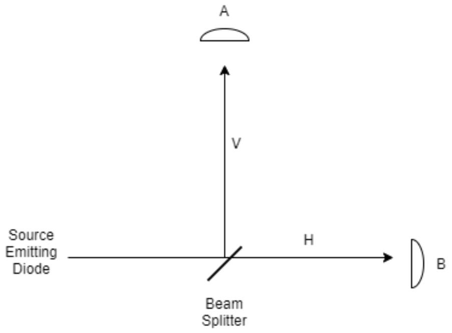


Figure 1: Beam Splitting

As seen in the above figure the light source emits a photon onto the half-silvered mirror. The mirror splits the light in such a way that half of the light is transmitted towards detector B and other half is reflected towards detector A. Since a single photon cannot be split as it has a single quantized energy state (hν), so it is detected with half probability at both A and B. This probability value is derived from the fact that when A has detected something then B does not and vice versa. Hence the probability is equally distributed between the two detectors. According to classical mechanics one may think that the given photon travels either vertically or horizontally randomly choosing between the two paths. However according to quantum mechanics, the photon actually travels both the paths simultaneously, collapsing to a given path that is horizontal or vertical upon measurement. This effect is known as the single-particle interference (refer appendix) resulting from the linear superposition of the possible states of the given two paths. The phenomenon is better explained with another experiment as shown in figure 2. In this experiment two beam splitters (refer appendix) and two fully silvered mirrors are used. A beam splitter is basically a half-polished mirror (half silvered mirror). As the first experiment shows the beam splitter splits the beam into two parts the transmitted part and the reflected part. In the second experiment the photon falls on a beam splitter. The two beams then recombine with the help of the fully silvered mirrors. Finally, the beam is again split with the help of a beam splitter before reaching the detectors. Each beam splitter introduces a 50% chance that the beam may go either way. Once the photon strikes the mirror in either way after the first splitter the later arrangement is similar to that of the first experiment. Thus, the photon travelling vertically when strikes the mirror should produce a 50% chance of getting detected at either A or B. The same happens for the photon moving along the horizontal direction. However, the actual results are drastically different. It is found that if the two possible paths are of the same length, then there is a 100% probability of photon reaching detector A and 0% probability of photon reaching detector B. It seems that it is inescapable for the photon to strike detector A, in some sense we can say that the photon has travelled both paths.

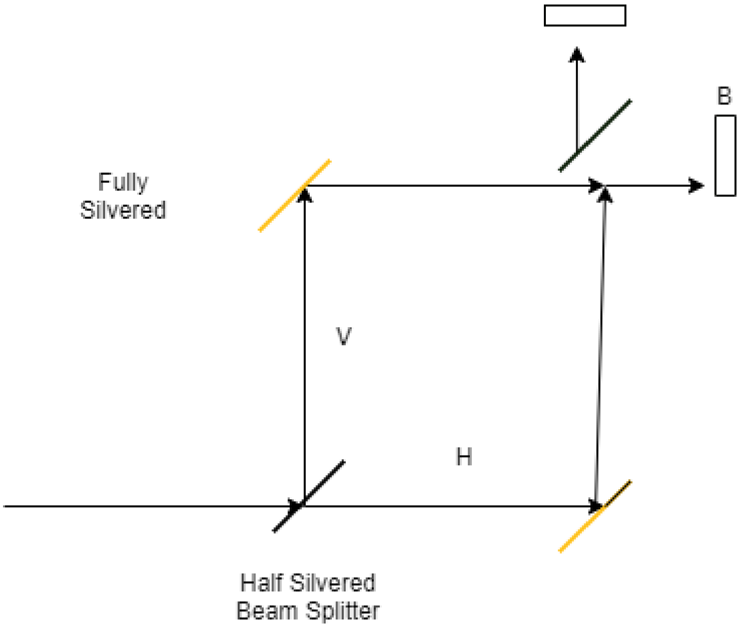


Figure 2: Wave-Particle Nature of Light

This phenomenon can be demonstrated by placing an absorbing screen in the way of either of the routes, then the photon becomes equally probable at detector A and B. When one of the paths are actually blocked the photon reaches detector B. With both the routes open the photon must have known that it cannot reach B so it must have travelled both paths. Hence it is justified to say that between the two beam splitters the photon exists in both the transmitted and reflected paths, or we can say that the photon is in a coherent superposition of being present in the transmitted beam and in reflected beam. This inference is due to linear superposition principle. This is the concept that make the research in quantum computing a rather new branch of thought. It is because quantum computers possess these unique characteristics that it gives them potential to be incredibly powerful computational device.

Quantum Entanglement

Classical physics help us to well describe the correlations existing in our day-to-day life. One of the basic examples of a day-to-day correlation can be presented with a simple example. Suppose we have a cat trapped in a box with food that has been poisoned. We know the correlation between the event of cat eating the food and the event of the cat's death. Hence there exists a correlation between the existence of the cat and whether the cat ate the food.

Such correlations that occur in the macroscopic world are easy to identify, but when it comes down to the microscopic world governed by the laws of quantum mechanics here, we see that such correlations are not easy to predict. A similar case to the cat example above is the condition of an atom that can undergo decay. So, we may predict it is either decayed state or not decayed state, but this is not the only two states it is found that the atom can also exist in a state that is in between these two states that is between decayed and not decayed. Just as discussed before this is due to the phenomenon of linear superposition of two quantum mechanical states of an atom. This is the situation when it comes to one atom, in the case of two atoms it is seen that if one of the atoms is decayed then the other is also decayed. This correlation exists even for the superposition state. Hence this is proof of 100% correlation between the state of the two atoms. This kind of super correlation is called **Quantum Entanglement** (refer appendix).

It was Edward Schrodinger who discovered this concept, he was the first to realize its weird characteristics. Suppose In the above given example the event of the cat eating the food was triggered by whether or not the nucleus has decayed. This means that if the decay happens the cat eats the food and dies, if the decay doesn't happen then the cat lives, else if the nucleus is in a superposition state, then the cat can be considered in a situation where it is both dead and alive. This is was indeed the very concept of 'The Schrodinger Cat'. The only difference is that instead of poisoned food there was a lethal chemical that would be released upon the nucleus decay. Such problems don't arise in everyday life and hence only when it comes to quantum mechanics we get to know of such phenomena.

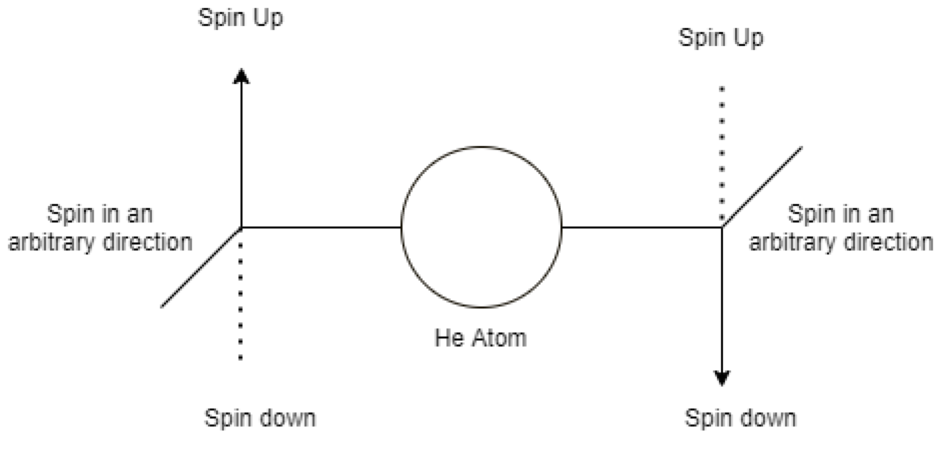

Spin Up
Spin Up
Spin in an arbitrary direction
Spin in an arbitrary direction
He Atom
Spin down
Spin down

Figure 1:*EPR Paradox Experiment*

The topic of quantum entanglement was briefly discussed in the paper published by Einstein, Podolsky and Rosen who believed that quantum mechanics is incomplete and not wrong. The paper they published brought into consideration the EPR **paradox** (refer appendix). The EPR paradox can be explained easily by the given experiment. Consider a He atom with just 2 electrons with quantum numbers n=1, l=0, s=1/2 and opposite spins. These two electrons in He are **antiparallel** (refer appendix) to each other and hence form an entangled pair. When the atom is provided sufficient energy, it disintegrates at rest and the two electrons fly away in opposite directions. The two electrons are taken apart. The real effect of the paradox is observed when a magnetic field is applied on one of the electrons causing its spin to be flipped. When this happens, it is observed that simultaneously the spin of the other electron is also flipped. This is the EPR paradox and it suggests a way of communication with the speed faster than that of light. The mechanism of this cannot be explained with surety, it is a simple theory that we must believe in.

This EPR paradox hence provides us with the idea of communication across space like events. Quantum Entanglement allows qubits separated by large distances to instantly interact with each other at a speed not even limited by the speed of light. The distance between the electrons doesn't matter as long as they are isolated. Hence together the concepts of quantum entanglement and quantum superposition does propose the creation of an enhanced computer with enormous computational power.

Bertlemann's Socks

There is another concept that introduces a new idea to the concept of quantum entanglement and this is the Bertlemann's socks. All such concepts are better explained through stories. Mr. Bertlemann always used to wear different pairs of socks and also, he used to wear only specific colour pair that is yellow-blue, red-green so on. He never breaks this order. So, if one can observe one of his socks then it is evident what colour the other is. This seems to be similar to a quantum entanglement situation but it is not. In quantum entanglement the choice of measurement plays an important role. There are many ways to measure the spin of an electron, the other particle arranges its spin accordingly. In the case of Bertlemanns Socks the onlooker plays this role of measurement selection. It is the onlooker that decides to see the one sock and predict the other.

EPR Situation, Bell Theorem and Hidden Variables:

John Bells analysis of the paper by Einstein, Podolsky and Rosen lead to contradictory conclusions. In his paper 'On the Einstein Podolsky Rosen Paradox' he introduces the Bells theorem that proves that quantum mechanics is incompatible with the local hidden variable's theories. According to the local hidden variable's theory the interpretation of quantum mechanics is a hidden variable theory that has the added requirement of consistency with **local realism** (refer appendix). According to Bells examination of 'Is Quantum Mechanics Complete?' by Einstein, Podolsky and Rosen he concluded that the EPR correlations also known as quantum entanglement have to be predicted by some supplementary parameters also called hidden variables. The above results demonstrated that the hidden variables description in fact contradicts some predictions of quantum mechanics. Because of these two contradictory theories there was no way to find out the truth.

An EPR Situation:

The experiment shown below uses a source that emits a pair of electrons v1 and v2 travelling in opposite directions. Each photon then falls onto a polarizer, which measures the linear **polarization** (refer appendix) along both the directions determined by orientation of the corresponding polarizer.

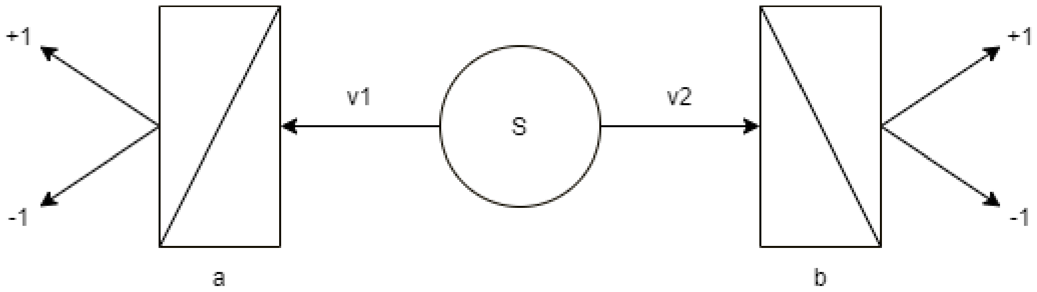


***Figure 2**: Graph Description of The EPR Situation*

Once the two photons come out of the polarizer there are two possible values for each measurement that is +1 or -1. Quantum mechanics allows the existence of a state of superposition (an EPR state) for which the measurements taken separately appear random but actually are strongly correlated. It is found that Probability (a, +1) and Probability (a, -1) for v1 is predicted to be 0.5 each, similar is the case for Probability (b, +1) and Probability (b, -1) independent of the orientation of b.

The probability for observing both + for both photons is given by 0.5Cos^2(a.b). If the polarizers are parallel then a. b=0, then we have probability 0.5. For cross polarizers a.b=pi/2, the probability is 0. The final results for the two photons of the same pair are hence, always identical which means there is complete correlation. Such correlations among events which appear random occur not only in physics but also in other fields. The basic conclusion derived by John Bell is that the natural generalization of the EPR reasoning leads to the assumption that quantum mechanics is not a final description of physical reality. The complete description of a pair must include a something in addition to the state vector, this something is the hidden variables.

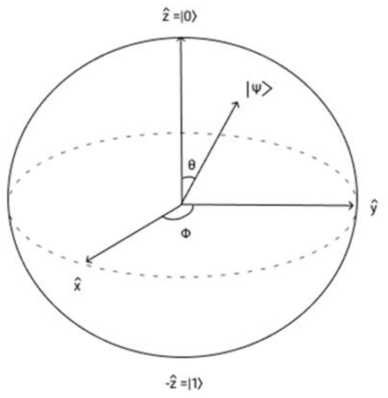
Bell Inequalities

Bell tried to predict the correlation between the two polarized states of a photon. Bell's inequalities basically concern about the measurements made by observers on pairs of particles that have interacted and then separated. In the above experiment the particle pair is photon and they have emerged from the same source meaning they have interacted and then they separated. The measurement made in the above experiment is the measurement of polarized states of the photons. According to Bell certain constraints must apply to the relationship between the correlation of the given two photon pairs. The polarized states of photon hence cannot take any set of value as some constraints apply to the correlation. If we consider the possible orientations as [(a.b),(a'.b),(a.b'),(a'.b')], the corresponding correlation coefficients are restricted by Bell inequalities according to which a give combination of these coefficients 's' is between -2 and +2 for any valid hidden variable theory. The value of s as predicted by quantum mechanics does not match the s value given by Bells inequalities. Bell inequalities basically describe a test for the validity of the hidden variable theory hence as the s value does not match, we can conclude that the hidden variable theory does not account of the EPR correlation predicted by Quantum Mechanics.

Bell inequality has the assumption of local hidden variable models as its foundation. According to the assumption of locality the result of a measurement by a polariser cannot be manipulated or influenced by the choice of the orientation of other remotely located polariser. This is an outcome of Einstein's rule that no signal can move with a speed greater than that of light. Bell inequalities also apply to other theories. Finally, any theory in which each photon has a reality localised in space time, determining any measurement will cause inequalities that will conflict with quantum mechanics. Thus, Bells Theorem can be finally phrased as 'Some quantum mechanical predictions cannot be copied by any local realistic model in Einstein's ideas of theory of hidden variables.

Requirement

Here, in this section, we consider on how to build a Quantum Computer. Similar to a classic computer a Quantum computer also require **Universal Gates,** which implement any legitimate quantum computation. There are five experimental requirements for building a quantum computer.



The Bloch sphere is a representation of a qubit, the fundamental building block of quantum computers.

Source: Wikipedia

https://en.wikipedia.org/wiki/Quantum_computing

The first requirement is the ability to compute quantum information efficiently. Second, a quantum computer requires the ability to set an initial state. This appears to be a main problem for most quantum systems because of the imperfect isolation from the environment and the difficulty of producing desired input states. Third, a quantum computer requires the need of a long decoherence time which should be much longer than the operation of gates. **Decoherence** is the coupling between qubit (two-level system) and its environment and this results in the loss of quantum phase coherence. After decoherence, quantum mechanical properties associated with coherence such as superposition and entanglement cannot be observed. The fourth requirement is the ability to measure output results from certain qubits. Generally, the output of a quantum algorithm is quantum superposition. Therefore, it is necessary to obtain result from quantum state using classical systems of very high fidelity. The fifth requirement is the ability to construct a universal set of quantum gates.

There have been several implementations of quantum computers. One of these include the Nuclear Magnetic Resonance (NMR). This Computer uses a vial of liquid-filled with sample molecules as qubits. An ion-trap based quantum computer uses a string of ions confined in a linear trap. Each ion represents a qubit and is manipulated by laser beams. A Cavity Quantum Electrodynamics (QED) based computer is schemed to use photons as qubits. A Quantum-dot-based quantum computer uses spins or energy levels of electrons that are confined in quantum dots as qubits that are further fabricated by semiconductor materials. Since we can control the states of qubits electrically, like we do in classical computers, this method has its advantage as the current semiconductor technology can be applied for the fabrication of the quantum computer. A Superconducting quantum computer uses the **Josephson-junctions** (refer appendix) in superconducting circuits as qubits.

Since it is extremely difficult to isolate quantum registers efficiently from their environments, a real quantum computer needs to be designed with by considering the effects of errors on the state of quantum registers. To protect the quantum states against the effects of noise several Quantum Error Correcting (QEC) schemes have been proposed. QEC codes are developed based on principles similar to classic error-correcting code.

Applications

Most algorithms need a larger number of high-quality qubits in order to be useful, most likely requiring quantum error correction-far beyond the available quantum resources. Also, the current inability to load large quantities of input data efficiently suggests that many of these applications would be difficult to implement in practice. Also, algorithms are not themselves applications; but they are basic elements that must be combined to perform a particular task.

The best example for an application of quantum algorithm is in the field of cryptography, an application which is based on mathematics. The potential near-term usage of a quantum computer is currently an area of active research as these are applications that require fewer qubits and can be implemented with a comparatively shallow code. The electronic structure problem, owing to the fields of chemistry and materials science, requires solving for the ground state energies and wave functions of electrons. Electronic structure defines chemical properties as well as the rates and products of chemical reactions. While classical computing approaches to this problem may be quite effective, they mostly fail to reach the given amount of accuracy. Quantum computer will provide efficient solutions to the above problem.

Another important aspect in the path of useful quantum computers is **Quantum Supremacy** (a demonstration of any quantum computation that is hard for a classical computer i.e., whether or not a computation is useful) (refer appendix). Quantum supremacy would address the viability of quantum computers as well as provide a test of quantum theory.

Challenges

A classical computer uses bits to represent the values during its operation, while a quantum computer uses what is called as **Quantum bits(qubits).** A bit can be either 0 or 1 but a qubit can represent values 0 or 1, or some combination of both simultaneously which is known as superposition. But a quantum computer can work in an exponentially larger problem space. Many innovations over the last 25 years have enabled researchers to build physical systems that provide the needed isolation and control for quantum computing. Even it is possible to make very high-quality qubits, creating and making use of these quantum computers is indeed challenging. These computers use a different set of operations than those of classical computers, requiring new algorithms, software, hardware and control technologies.

1) Rejection of noise by qubits is not possible intrinsically

   One of the main differences between a classical and quantum computer is how these handle unwanted small variations, or noise in the system. Since a qubit is a combination of one and zero, qubits and quantum gates cannot readily reject small errors or noise that occur in the physical circuits. So, one of the most significant design parameters for those systems which operate on physical qubits is their error rates.

2) Loading of Large Data Inputs

   While a quantum computer can use a small number of qubits to represent an exponentially larger quantity of data, presently there is not a method to rapidly convert large amount of classical data to a quantum state. As a consequence, the amount of time needed to create the quantum input state would typically dominate the computation time, reducing the quantum advantage.

3) Quantum Error Correction required for Error-Free quantum computer

   Although, the physical qubit operations are much sensitive to noise, it is possible to carry out a Quantum error correction (QEC) algorithm in a physical computer to emulate a noise-free quantum computer. While QEC's might be essential to create error-free quantum computer, they are too resource intensive to be used in short-term.

4) Quantum Algorithm design is Challenging

   One can extract exactly the same amount of data from a quantum computer that one can do from a physical computer of the same magnitude. To receive the benefits of a quantum computer, quantum algorithm must leverage uniquely quantum features to arrive the final classical result. So, achieving quantum speeding up requires fully new kinds of algorithms and very clever algorithm designs

5) Intermediate State of a quantum computer is difficult to be measured

   The debugging methods for classical Computer rely on memory, and reading of intermediate machine states; which is both not possible in a quantum computer. A quantum state cannot be copied simply for later evaluation. New approaches to debugging are crucial for the development of large-scale quantum computers.

6) Necessity of a Software Stack for Quantum Computers

   As quantum programs are different from programs for classical computers, development and research is needed for further development of the software tool stack. As these software tools drive the hardware, the development of both hardware and software tools will definitely shorten the time for these quantum computers.

Thermodynamics

Based on the laws of thermodynamics, computers are also subject to thermodynamic constraint. Computers are machines so, like all machines they are all subject to thermodynamic constraints. Similar to any physical system, modern computers based on digital devices, also produce heat in operation. It is important of an ideal computer capable of shaping, maintaining and moving around digital signals, without any heat generation. But there is one place where heat is produced, when information is erased, the phase space associated with the system that stores the information shrinks. Removing a single bit of information reduces entropy of the system that stored the information. This reduction of entropy causes the heat release to the environment. Thus, if a computer can be constructed that does not remove any information, such a computer could work without generating any heat at. This is the situation in quantum computers. Quantum Computation is a reversible process. It is therefore possible in principle, to carry out quantum computation without generating heat. But, in reality the computer would definitely generate a lot of heat because of electric pulses moving across copper wires and their emission of heat due to resistance. The reversibility capability of quantum computers is realized by conceiving special gates. For the construction of digital computers, NOR, AND, NAND and XOR gates are used which are irreversible gates and these generate heat.

$$(a,b) \longrightarrow (a \wedge b)$$

Here the amount of information on the right-hand side of the equation is less than the amount on left-hand side. Using Toffoli Gates, it can be demonstrated that quantum computers are capable of carrying out computation using reversible steps alone.

Realization of Quantum Computers experimentally

The architectural simplicity makes quantum computer faster, cheaper and smaller, but its conceptual complexity is severe problems for its experimental realization. Moreover, some attempts have been made in this direction by encouraging success. It is realized that it may not be too long when the quantum computer could replace the digital Computer with its full realization. Some of the attributes for the experimental realization of a quantum computer are summarized as follows:

Ion Traps:

An ion trap quantum computer was implemented first by Monroe and collaborators in 1995 followed by Schwarzschild in the year 1996. The ion trap computer uses encodings of data in energy states of ions as well as vibrational modes between the ions. Theoretically, each ion is operated by a laser. A fundamental analysis demonstrated that Fourier transforms can be examined with the ion trap type of Computer. This leads to Shor's factoring algorithm, which is mainly based on Fourier transforms.

Quantum Electrodynamics Cavity:

Quantum electrodynamics (QED) cavity computer was first demonstrated by Hette and collaborators in 1995. The computer contains of a QED cavity filled with some cesium atoms and an arrangement of lasers, phase shift detectors, polarizer and mirrors. The setup is an actual quantum computer because it can create, manipulate and preserve superposition and entanglements.

Quantum Dots:

Quantum computers which are based on quantum dot technology use much simpler architecture and more sophisticated experimental, mathematical and theoretical skills in comparison to the quantum computer implementations discussed so far. An array of quantum dots, where the dots are connected with the nearest neighbors by means of gated tunnelling barriers are used for fabricating quantum gates using the split-gate technique. This scheme has one of the primary advantages: the qubits are mainly controlled electrically. The main disadvantage of this architecture is that quantum dots can communicate with their nearest neighbors only resulting data readout is quite tricky.

Josephson Junctions

The Josephson junction quantum computer was demonstrated in 1999 by Nakamura and co-workers. In this Computer, a Cooper pair box, which is a small superconducting island electrode is weakly coupled to a bulk superconductor. Weak coupling between the superconductors creates a Josephson junction between them which behaves as a capacitor. If the Cooper box is as small as a quantum dot, the charging current breaks into a discrete transfer of separate Cooper pairs, so that ultimately it is possible to transfer a single Cooper pair across the junction. Like quantum dot, computers in Josephson junction computers also, qubits are controlled mainly electrically. Josephson junction's quantum computers are among much needed candidates for future developments.

Future Directions of Quantum Computing

The bases for the subject of quantum computation have become well developed, but the remaining technology required for its future growth is still under development. This includes quantum algorithms, understanding the dynamics and control of decoherence. Reversibility of quantum computation may assist in solving problems which are simple in one direction and difficult in the other sense.

Quantum Field Theory (refer appendix) can extend quantum computation to allow the creation and destruction of quanta. The very natural setting for such an operation is quantum optics. The **Double slit experiment** (refer appendix) is permitted in quantum operation because the intensity of two copies is half the previous value. Though its dynamics is not well-understood **Decoherence** (refer appendix) can described as an effective process. In order to control decoherence, one should be able to figure out the eigen states favored by the environment in the setup. The dynamics of measurement process is also not understood either. Measurement is described as a non-unitary projector operator. Ultimately, both the system and the observer are made of quantum building blocks, and a unified quantum description of both measurements need to be developed. It is important to study the transition from classical to quantum systems. Enlargement of the system from microscopic to mesoscopic levels and its reduction from macroscopic to mesoscopic levels can take us there to the target.

Theoretical developments alone will be no use without a corresponding technology. In the present day, the miniaturization of electronic circuits is not much away from quantum reality of nature. To devise new instruments, we must change our view-point from scientific to technological-quantum effects. It is true that the future world sees a more practical usage of quantum computers.

Quantum Machine Learning

The field of quantum computing has a lot to contribute to several domains like optimization, quantum simulation, cryptography, machine learning. One of the most important one's being the field of Quantum Machine Learning. Quantum Machine Learning is the integration of quantum algorithms with machine learning programs. There are 2 important terms in focus, quantum algorithms and machine learning. Quantum algorithm are algorithms that run on a realistic model of quantum computation, which is the quantum circuit model of computation. The latter term machine learning is basically using data to predict data and forecast data.

Quantum computing can help scale down the amount of time taken to train a machine learning model by an exponential factor. The same has been proved by Google's quantum beyond-classical experiment which used 53 qubits to demonstrate it could perform a calculation in 200s on a quantum computer which otherwise would have taken 10000 years on the largest classical computers we possess.

As discussed above Quantum Computing relies on the abilities of qubits to be put into superposition and share entanglement with one another. Classical computers perform deterministic operations, but by harnessing the ability of superposition and entanglement quantum computers can perform quantum operations that are difficult to emulate at scale with classical computers.

Just like any machine learning model, even quantum machine learning requires data and a model, algo to build on the provided data. This in the case of quantum machine learning is quantum data and hybrid quantum classical models.

Quantum Data

Quantum data is the data source that occurs in a natural or artificial quantum system, data generated by a quantum computer is an example of such data. Quantum data exhibits the properties of superposition and entanglement leading to joint probability distributions that could require exponential amount of classical computational resources to store. The Noisy Intermediate Scale Quantum generates data that are noisy and typically entangles just before the measurements occurs, thus making them a little more interpretable. Heuristic machine learning models can be developed on this noisy entangles data to extract useful classical data. To our surprise there are several projects that aim at transforming quantum data received from NSIQ, one such being the TensorFlow Quantum library (TFQ) which provides methods to develop models that disentangle and generalize correlations in quantum data.

Hybrid Quantum-Classical Models

A quantum model can represent and generalize, correlate data from a quantum mechanical origin. The current quantum processors we possess are still small and noisy thus making us depend on the need for NISQ processors to work with classical co-processors to become effective. TensorFlow being a platform that supports heterogenous computing across CPUs, GPUs, TPUs, it is used as a base platform to experiment with hybrid quantum-classical algorithm.

III. CONCLUSION

In this paper, we have provided an introduction to the world of Quantum computing and the future importance of the field. We have analyzed the field of quantum computing by providing details from the beginning of the field until now where we are overlooking into the field for more reasonable applications. The field has its own benefits in terms of accuracy and precision but also has its own limitations considering the present circumstances of the technology. But the development of this field will indeed be of immense importance to the world of Computer and those working in it!

IV. REFERENCES

Main source:

- A Study on the basics of Quantum Computing, Department d'Informatique et de recherché operationnelle, Universite de Montreal. The given research paper is a reinterpretation of the given research paper. The diagrams taken have been modified.

Other Sources:

- Wikipedia - Bells Theorem, EPR Paradox
- Research Gate
- Scholarpedia
- link.springer.com
- hackaday.com
- *https://en.wikipedia.org/wiki/Parallel_computing*
- *Archil Avaliani,International University,December 1, 2002,Quantum Computers*

{Daniel, G. (1999). Quantum Error-Correcting Codes. Retrieved on November 31st,

2002 from: http://qso.lanl.gov/~gottesma/QECC.html

Manay, K. (1998). Quantum computers could be a billion times faster than Pentium

III. USA Today. Retrieved on December 1st, 2002 from:

http://www.amd1.com/quantum_computers.html

Quantum Computers. Retrieved on December 1st, 2002 from:

http://www.ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm

Quantum Computers & Moore's Law. Retrieved on December 1st, 2002 from:

http://www.qubyte.com

Quantum Computers: What are They and What Do They Mean to Us? Retrieved on

December 1st, 2002 from:

http://www.carolla.com/quantum/QuantumComputers.htm

West, J (2000). Quantum Computers. Retrieved December 1, 2002 from California

Institute of Technology, educational website:

http://www.cs.caltech.edu/~westside/quantum-intro.html#qc}

- *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2018 Symposium.*
- *8803 Machine Learning Theory*
- *Maria-Florina Balcan Lecture 4: September 1st, 2011*

V. APPENDIX

- **Mistake bound model:** An algorithm A is said to learn C in the mistake bound model if for any concept c ∈ C, and for ordering of examples consistent with c, the total number of mistakes ever made by A is bounded by p(n, size(c)), where p is any polynomial.
- **Qubit:** A qubit is the basic unit of quantum information.
- **Superposition:** It is a principle that states that the resultant response caused by two or more stimuli is the total sum of the responses that might have been caused by each stimulus individually.
- **Eigenstates:** A quantum mechanical state corresponding to an eigenvalue.
- **Polarization:** A property that clarifies the geometrical orientation of the oscillation.
- **Interference**: In terms of waves, it is the combination of two or more electromagnetic waves to form a resultant displacement.
- **Beam Splitter**: Optical device that splits beam of light into two. Extensively used in telecommunication.
- **Entanglement**: A complicated or comprising relationship or situation.
- **Antiparallel:** Parallel but moving or oriented in opposite directions
- **Paradox:** A seemingly contradictory statement or proposition which when investigated may prove to be well founded or true.
- **Local Realism**: It is basically a premise (or accurately a combination of two premises) introduced by Einstein, Podolsky, Rosen.
- **Quantum Supremacy**: In terms of quantum computing, quantum supremacy is the target of demonstrating that a programmable quantum device can solve a problem which no classical computer can feasibly solve.
- **The Schrödinger Cat:** It is a thought experiment sometimes also considered as a paradox, devised by Erwin Schrodinger in 1935.
- **Josephson-junctions:** The Josephson effect is the phenomenon of supercurrent, a current that flows indefinitely without any voltage applied, across a device which is known as a Josephson junction, which consists of two or more superconductors which is coupled by a weak link.
- **Decoherence:** It can be viewed as the loss of information from a system into the environment, since every system is loosely coupled with its surroundings.
- **Quantum Field Theory:** In theoretical physics, quantum field theory can be defined as a theoretical framework that combines classical field theory, quantum mechanics and special relativity but not general relativity's description of gravity.
- **Double slit experiment:** The double-slit experiment is a demonstration that light as well as matter can display characteristics of both classically defined waves as well as particles.
- **Universal Gates**: A universal gate is a gate which can implement any Boolean function without using any other gate type.