A REPORT ON QUANTUM COMPUTING

Achintya A. Paradkar[1] **and Vipul V. Joshi**[2]
[1,2] Singhad Academy of Engineering, Pune, India
achintyaparadkar@gmail.com

Abstract

Today's computers work on bits that exist as either 0 or 1. Quantum computers aren't limited to two states; they encode information as quantum bits, or qubits, which can exist in superposition. Qubits represent atoms, ions, photons or electrons and their respective control devices that are working together to act as computer memory and a processor. Because a quantum computer can contain these multiple states simultaneously, it has the potential to be millions of times more powerful than today's most powerful supercomputers. A processor that can use registers of qubits will be able to perform calculations using all the possible values of the input registers simultaneously. This superposition causes a phenomenon called quantum parallelism, and is the motivating force behind the research being carried out in quantum computing.

Due to technical obstacles, till date, a quantum computer has not yet been realized. But the concepts and ideas of quantum computing has been demonstrated using various methods like NMR, Ion Trap, Quantum Dot, Optical Methods, etc. A quantum computer manipulates qubits by executing a series of quantum gates, each a unitary transformation acting on a single qubit or pair of qubits. In applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits in some initial state. The qubits can then be measured, with this measurement serving as the final computational result.

Research must devise a way to maintain decoherence and other potential sources of error at an acceptable level. Probably the most important idea in this field is the application of error correction in phase coherence as a means to extract information and reduce error in a quantum system without actually measuring that system. Thereby, quantum computers will emerge as the superior computational devices and perhaps one day make today's modern computer obsolete.

Keyword*s* – Qubits, superposition, parallelism, coherence, entanglement, quantum gates, decoherence, NMR, quantum dots.

1. INTRODUCTION TO QUANTUM COMPUTERS

Gershenfeld says that if making transistors smaller and smaller is continued with the same rate as in the past years, then by the year of 2020, the width of a wire in a computer chip will be no more than a size of a single atom. These are sizes for which rules of classical physics no longer apply. If the transistors become much smaller, the strange effects of quantum mechanics will begin to hinder their performance.

In 1982, the Nobel prize-winning physicist Richard Feynman thought up the idea of a 'quantum computer', a computer that uses the effects of quantum mechanics to its advantage. For some time, the notion of a quantum computer was primarily of theoretical interest only, but recent developments have bought the idea to everybody's attention. One such development was the invention of an algorithm to factor large numbers on a quantum computer, by Peter Shor (Bell Laboratories). By using this algorithm, a quantum computer would be able to crack codes much more quickly than any ordinary (or classical) computer could. In fact a quantum computer capable of performing Shor's algorithm would be able to break current cryptography techniques in a matter of seconds. With the motivation provided by this algorithm, the topic of quantum computing has gathered momentum and researchers around the world are racing to be the first to create a practical quantum computer.

According to Chuang a supercomputer needs about a month to find a phone number from the database consisting of world's phone books, where a quantum computer is able to solve this task in 27 minutes. Massachusetts Institute of Technology, Oxford University, IBM and Los Alamos National Laboratory are the most successful in development of quantum computer.

2. NEED OF QUANTUM COMPUTER

2.1 The Potential and Power of Quantum Computing

Quantum computer with 500 qubits gives 2^{500} superposition states. Each state would be classically equivalent to a single list of 500 1's and 0's. Such computer could operate on 2^{500} states simultaneously. Eventually, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. This kind of computer is equivalent to a classical computer with approximately 10^{150} processors.

Integer factorization is believed to be computationally infeasible with an ordinary computer for large integers if they are the product of few prime numbers (e.g., products of two 300-digit primes). By comparison, a quantum computer could efficiently solve this problem using Shor's algorithm to find its factors. This ability would allow a quantum computer to decrypt many of the cryptographic systems in use today. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers. These are used to protect secure Web pages, encrypted email, and many other types of data. Breaking these would have significant ramifications for electronic privacy and security. An example of this is a password cracker that attempts to guess the password for an encrypted file (assuming that the password has a maximum possible length).

2.2 Moore's Law for Quantum Computers

According to Moore's Law, the number of transistors of a microprocessor continues to double in every 18 months. According to such evolution if there is a classical computer in year 2020, it will run at 40 GHz CPU speed with 160 GB RAM. If we use an analogue of Moor's law for quantum computers, the number of quantum bits would be double in every 18 months. But adding just one qubit is already enough to double a speed. So, the speed of quantum computer will increase more than just doubling it.

2.3 The Major Difference between Quantum and Classical Computers

The memory of a classical computer is a string of 0s and 1s, and it can perform calculations on only one set of numbers simultaneously. The memory of a quantum computer is a quantum state that can be a superposition of different numbers. A quantum computer can do an arbitrary reversible classical computation on all the numbers simultaneously. Performing a computation on many different numbers at the same time and then interfering all the results to get a single answer, makes a quantum computer much powerful than a classical one.

2.4 Superiority of Quantum Computer over Classical Computer

These are the most important applications currently known:

- Cryptography: Perfectly secure communication.
- Searching, especially algorithmic searching (Grover's algorithm).
- Factorizing large numbers very rapidly (Shor's algorithm).
- Simulating quantum-mechanical systems efficiently.

3. QUANTUM COMPUTER BASICS

In the classical model of a computer, the most fundamental building block, the bit, can only exist in one of two distinct states, a 0 or a 1. In a quantum computer the rules are changed. Not only can a 'quantum bit', usually referred to as a 'qubit', exist in the classical 0 and 1 states, it can also be in a coherent superposition of both. When a qubit is in this state it can be thought of as existing in two universes, as a 0 in one universe and as a 1 in the other. An operation on such a qubit effectively acts on both values at the same time. The significant point being that by performing the single operation on the qubit, we have performed the operation on two different values. Likewise, a two-qubit system would perform the operation on 4 values, and a three-qubit system on eight. Increasing the number of qubits therefore exponentially increases the 'quantum parallelism' we can obtain with the system. With the correct type of algorithm it is possible to use this parallelism to solve certain problems in a fraction of the time taken by a classical computer.

The characteristic feature of quantum computing is quantum parallelism. A quantum system is in general not in one "classical state", but in a "quantum state" consisting (crudely speaking) of a superposition of many classical or classical-like states. Superposition does not mean we could drop all but one of the classical-like states (after deducing retrospectively which one was "the right one") and still get the time evolution right. But actually we need the whole superposition to get the time evolution right. The system really is in some sense in all the classical-like states at once! If the superposition can be protected from unwanted entanglement with its environment (known as decoherence), a quantum computer can output results dependent on details of all its classical-like states. This is quantum parallelism - parallelism on a serial machine.

But unlike classical bits, qubits can exist simultaneously as o and 1, with the probability for each state given by a numerical coefficient; describing a two-qubit quantum computer thus requires four coefficients. In general, n qubits demand 2^n numbers, which rapidly becomes a sizable set for larger values of n. For example, if n equals 50, about 2^{15} numbers are required to describe all the probabilities for all the possible states of a quantum machine – a number that exceeds the capacity of the largest conventional computer, a quantum computer promises to be immensely powerful because it can be in multiple states at once-a phenomenon called superposition—and because it can act on all its possible states simultaneously. Thus a quantum computer could naturally perform myriad operations in parallel, using a single processing unit.

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 measurement of all the states, collapsing each qubit into one of the two pure states, so the outcome can be at most classical bits of information.

In order to do this we use certain Quantum Mechanical concepts like:

1) Superposition
2) Entanglement
3) Parallelism

3.1 Coherent Superposition

In any quantum mechanical system, a particular state of the system is represented by a mathematical function called as the wave function of that state. A wave function is a complex exponential which includes all possible phases of existence of that particular state.

Considering any quantum mechanical system, let ψ1 and ψ2 be two wave functions that represent any two independent states of the system. Then quantum mechanics tells us that there exists a state of the same system that can be represented by the wave function c1ψ1 + c2ψ2. This state is called as a superposition of the two states represented by ψ1 and ψ2. It means that the system would be in both the states of ψ1 and ψ2 simultaneously.

All superposition of two quantum states of a system are not stable. If the superposition is to be stable, then there should be some sort of coherence between the two states that are being superpositioned. Such a superposition is called as a coherent superposition. There can be more than one coherent superposition for a pair of states of a quantum mechanical system.

3.2 Advantage of Using Coherent-Superpositioned Memory

The importance of coherent-superpositioned storage can be understood from the following example. Consider a register composed of three physical bits. Any classical register of that type can store in a given moment of time only one out of eight different numbers i.e. the register can be in only one out of eight possible configurations such as 000, 001, 010, ... 111. Consider the case of a quantum register at that place.

Since a qubit can store both the values of 0 & 1 simultaneously, a quantum register composed of three qubits can store in a given moment of time all the eight numbers in a quantum superposition. The catch is that the memory size grows exponentially when additional bits are added compared to the linear growth in classical computers. Also, once the register is prepared in such a superposition, operations can be performed on all the numbers simultaneously.

3.3 Role of Coherent Superposition in Computing Operations

We have seen that once a register is prepared in a superposition of different numbers, we can perform operations on all of them. For example, if qubits are atoms then suitably tuned laser pulses affect atomic electronic states and evolve initial superposition of encoded numbers into different superposition. During such evolution each number in the superposition is affected and as the result we generate a massive parallel computation albeit in one piece of quantum hardware. This means that a quantum computer can in only one computational step perform the same mathematical operation on 2L different input numbers encoded in coherent superposition of L qubits. In order to accomplish the same task, any classical computer has to repeat the same computation 2L times or one has to use 2L different processors working in parallel. In other words a quantum computer offers an enormous gain in the use of computational resources such as time and memory.

4. CONCEPT OF INFORMATION IN QUANTUM COMPUTERS – THE QUBIT

In quantum computers also, the basic unit of information is a bit. The concept of quantum computing first arose when the use of an atom as a bit was suggested. If we choose an atom as a physical bit then quantum mechanics tells us that apart from the two distinct electronic states (the excited state and the ground state), the atom can be also prepared in what is known as a coherent superposition of the two states. This means that the atom can be both in state 0 and state 1 simultaneously. It is at this point that the concept of a quantum bit or a qubit arises. This concept is the backbone of the idea of quantum computing. A quantum computer with a given number of qubits is fundamentally different from a classical computer composed of the same number of classical bits. For example, to represent the state of an n-qubit system on a classical computer would require the storage of 2n complex coefficients. Qubits are made up of controlled particles and the means of control (e.g. devices that trap particles and switch them from one state to another).

5. POSTULATES OF QUANTUM COMPUTING

An important distinction needs to be made between quantum mechanics, quantum physics and quantum computing. Quantum mechanics is a mathematical language, much like calculus. Just as classical physics uses calculus to explain nature, quantum physics uses quantum mechanics to explain nature. As classical computers can be thought of in Boolean algebra terms, quantum computers are reasoned about with quantum mechanics. There are four postulates to quantum mechanics, which will form the basis of quantum computers:

Postulate 1: Definition of a quantum bit, or qubit.
Postulate 2: How qubit(s) transform (evolve).
Postulate 3: The effect of measurement.
Postulate 4: How qubits combine together into systems of qubits.

6. OPERATION

While a classical three-bit state and a quantum three-qubit state are both eight-dimensional vectors, they are manipulated quite differently for classical or quantum computation. For computing in either case, the system must be initialized, for example into the all-zeros string, corresponding to the vector (1,0,0,0,0,0,0,0).

Finally, upon termination of the algorithm, the result needs to be read off. In the case of a classical computer, we sample from the probability distribution on the three-bit register to obtain one definite three-bit string, say 000. Quantum mechanically, we measure the three-qubit state, which is equivalent to collapsing the quantum state down to a classical distribution, followed by sampling from that distribution. Note that this destroys the original quantum state. Many algorithms will only give the correct answer with a certain probability. However, by repeatedly initializing, running and measuring the quantum computer, the probability of getting the correct answer can be increased.

7. DEMONSTRATING QUANTUM COMPUTING

Due to technical obstacles, till date, a quantum computer has not yet been realized. But the concepts and ideas of quantum computing has been demonstrated using various methods. Here, are four most important technologies used to demonstrate quantum computing:

7.1 Nuclear Magnetic Resonance

Using nuclear magnetic resonance (NMR) techniques, invented in the 1940's and widely used in chemistry and medicine today, these spins can be manipulated, initialized and measured. Most NMR applications treat spins as little "bar magnets", whereas in reality, the naturally well-isolated nuclei are non-classical objects. The spin manipulation is accomplished by application of magnetic pulses within a magnetic field produced by the NMR chamber.

The latest development in quantum computing takes a radical new approach. It drops the assumption that the quantum medium has to be tiny and isolated from its surroundings and instead uses a sea of molecules to store the information. When held in a magnetic field, each nucleus within a molecule spins in a certain direction, which can be used to describe its state; spinning upwards can signify a 1 and spinning down, a 0. Nuclear Magnetic Resonance (NMR) techniques can be used to detect these spin states and bursts of specific radio waves can flip the nuclei from spinning up (1) to spinning down (0) and vice-versa.

In this manner small-scale quantum algorithms have been experimentally demonstrated with molecules such as Alanine, an amino acid. This includes the quantum search algorithm, and a predecessor to the quantum factoring algorithm. The major drawback of this method is scalability; the signal strength of answer decreases exponentially with the number of qubits.

7.2 Ion Trap

An Ion Trap quantum computer is also based on control of nuclear spin (although using vibration modes or "phonons" has also been considered). In this approach the individual ions are, as the name implies, trapped or isolated by means of an electromagnetic field which is produced by means of an electromagnetic chamber. The trapped ions are cooled to the point where motion is essentially eliminated. They are then manipulated by laser pulses and a qubit arises from the superposition of lower and higher energy spin states. This technique is potentially scalable, but a great disadvantage is that it requires a cryogenic environment - not to mention that to date no more than single qubit systems have been demonstrated.

7.3 Quantum Dot

An example of an implementation of the qubit is the 'quantum dot' which is basically a single electron trapped inside a cage of atoms. A quantum dot is a particle of matter so small that the addition or removal of an electron changes its properties in some useful way. When the dot is exposed to a pulse of laser light of precisely the right wavelength and duration, the electron is raised to an excited state: a second burst of laser light causes the electron to fall back to its ground state. The ground and excited states of the electron can be thought of as the 0 and 1 states of the qubit and the application of the laser light can be regarded as a controlled NOT function as it knocks the qubit from 0 to 1 or from ' to 0.

If the pulse of laser light is only half the duration of that required for the NOT function, the electron is placed in a superposition of both ground and excited states simultaneously, this being the equivalent of the coherent state of the qubit. More complex logic functions can be modeled using quantum dots arranged in pairs. Unfortunately there are a number of practical problems that are preventing this from happening. The electron only remains in its excited state for about a microsecond before it falls to the ground state. Constructing quantum dots is a very difficult process because they are so small. A typical quantum dot measures just 10 atoms (1 nanometer) across.

A Quantum Dot quantum computer can involve manipulation of electrical charge, spin, or energy state - the Australians have a patent on a spin based version. A computer would be made up of a regular array of such dots. As with the prior two methods, the most popular approach is to have spin up counted as zero, spin down counted as one, and use a superposition of spin states to create the qubit. Techniques for self-assembly of large arrays of quantum dots have already been demonstrated and can be done using the industry standard silicon substrate.

7.4 Optical Method

As the name indicates, an optical quantum computer uses the two different polarizations of a light beam to represent two logical states. As an example, we can consider the polarization of a light beam in the vertical plane to represent a logical 1 and the polarization of the beam in the horizontal plane to represent a logical 0. An Optical quantum computer would be based on manipulating the polarization of individual photons. Entanglement is achieved by coincident creation of identical photons. Identical photons in this context would mean photons having the same energy as well as same polarization. The superposition of polarization or phase state is manipulated using polarizing lenses, phase shifters, and beam splitters.

7.5 Computing liquids

The quantum computer in this technique is the molecule itself and its qubits are the nuclei within the molecule. This technique does not however use a single molecule to perform the computations; it instead uses a whole 'mug' of liquid molecules. The advantage of this is that even though the molecules of the liquid bump into one another, the spin states of the nuclei within each molecule remain unchanged. Decoherence is still a problem, but the time before the decoherence sets in is much longer than in any other technique so far. Researchers believe a few thousand primitive logic operations should be possible within time it takes the qubits to decohere. Advancing beyond a 10-qubit system may prove to be more difficult. In a given sample of 'computing liquid' there will be a roughly even number of up and down spin states but a small excess of spin in one direction will exist. It is the signal from this small amount of extra spin, behaving as if it were a single molecule that can be detected and manipulated to perform calculations while the rest of the spins will effectively cancel each other out. This signal is extremely weak and grows weaker by a factor of roughly 2 for every qubit that is added. This imposes a limit on the number of qubits a system may have as the readable output will be harder to detect.

8. OBTAINING A RESULT

Once a calculation that makes use of quantum parallelism has been performed, there will be any number of different results in different universes. The fact that the results are not in this universe means that we can only obtain a solution to a computation by looking at the interference of the various results. It is important to note that looking at the result (or any intermediate state) of a quantum computer prevents any further interference between the different versions from taking place, i.e. prevents any useful quantum computations from continuing.

Such interference is best illustrated with a simple example; In Young's two slit experiment, light is shone through two parallel slits onto a screen. The resulting pattern of light and dark fringes displayed on the screen is a result of constructive and destructive interference. In a similar way, the results from each universe's calculation will constructively and destructively interfere to give a measurable result. This result has a different significance for different algorithms, and can be used to deduce the solution to the problem in hand.

9. REVERSIBLE COMPUTATION

What are the difficulties in trying to build a classical computing machine on such a small scale? One of the biggest problems with the program of miniaturizing conventional computers is the difficulty of dissipated heat. As early as 1961 Landauer studied the physical limitations placed on computation from dissipation .Surprisingly, he was able to show that almost all operations required in computation could be performed in a reversible manner, thus dissipating no heat! The first condition for any deterministic device to be reversible is that its input and output be uniquely retrievable from each other. This is called logical reversibility.

If, in addition to being logically reversible, a device can actually run backwards then it is called physically reversible and the second law of thermodynamics guarantees that it dissipates no heat. The work on classical, reversible computation has laid the foundation for the development of quantum mechanical computers. On a quantum computer, programs are executed by unitary evolution of an input that is given by the state of the system.

10. PROBLEMS IN PRODUCTION OF QUANTUM COMPUTERS

Any kind of measurement of quantum state parameters considers interaction process with environment (with other particles - particle of light for example), which causes a change of some parameters of this quantum state. Measurement of superposition quantum state will collapse it into a classical state. This is called de-coherence. This is the major obstacle in a process of producing of a quantum computer. If de-coherence problem cannot be solved, a quantum computer will be no better than a silicon one. In order to make quantum computers powerful, many operations must be performed before quantum coherence is lost. It can be impossible to construct a quantum computer that will make calculations before de-cohering. But if one makes a quantum computer, where the number of errors is low enough, than it is possible to use an error-correcting code for preventing data loses even when qubits in the computer de-cohere. Another problem is hardware for quantum computers. Nuclear Magnetic Resonance (NMR) technology is the most popular today, because of some successful experiments. MIT and Los Alamos National Laboratory have constructed a simple quantum computer using NMR technology. Some other designs are based on ion trap and quantum electrodynamics (QED). All of these methods have significant limitations.

11. OBSTACLES AND RESEARCH

The field of quantum information processing has made numerous promising advancements since its conception, including the building of two- and three-qubit quantum computers capable of some simple arithmetic and data sorting. However, a few potentially large obstacles still remain that prevent us from "just building one", or more precisely, building a quantum computer that can rival today's modern digital computer. Among these difficulties, error correction, decoherence, and hardware architecture are probably the most formidable.

11.1 Decoherence

Consider a qubit that is in the coherent state. As soon as it measurable interacts with the environment it will decohere and fall into one of the two classical states. This is the problem of decoherence and is a stumbling block for quantum computers as the potential power of quantum computers depends on the quantum parallelism brought about by the coherent state. This problem is compounded by the fact that even looking at a qubit can cause it to decohere, making the process of obtaining a solution from a quantum computer just as difficult as performing the calculation itself. We have seen that if a superposition of any two states of a quantum – mechanical system is to be stable over a period of time, there should be some sort of coherence between the states that are being superpositioned. For the same reason, no quantum memory can, at present, be used to hold data that is to be used for operations that take a long time. The time taken by the system to lose the coherence between the two states is known as decoherence time.

11.2 Error Correction

Error correction is rather self-explanatory, but what errors need correction?

The answer is primarily those errors that arise as a direct result of decoherence, or the tendency of a quantum computer to decay from a given quantum state into an incoherent state as it interacts, or entangles, with the state of the environment. These interactions between the environment and qubits are unavoidable, and induce the breakdown of information stored in the quantum computer, and thus errors in computation. Before any quantum computer will be capable of solving hard problems, research must devise a way to maintain decoherence and other potential sources of error at an acceptable level.

There are a lot of error-correcting codes. One of the simplest classical error-correcting codes is called repetition code. 0 is encoded as 000 and 1 as 111. Then if only one bit is flipped, one gets a state for example 011 that can be corrected to its original state 111. The signs of states in a quantum superposition are also important, but sign errors can also be corrected.

11.3 Lack of Reliable Reading Mechanism

The techniques that exist till date have a big problem that trying to read from a superpositioned qubit would invariably make it to lose its superpositioned state and make it to behave just as a classical bit – i.e. it would store only one among the values of 0 and 1.

Also, if we are given a quantum register comprising of n bits of which m bits are superpositioned ones, none among the reading mechanisms available today is able to determine which value from the superposition is to be read out. i.e. if we are given a 3 – bit register that contains, say, 4 values in a particular superposition (let them be 4,5,6,7), the reading mechanisms available today are unable to determine which how to access a specific value from the superposition.

12. APPLICATIONS OF QUANTUM COMPUTERS

It is important to note that a quantum computer will not necessarily outperform a classical computer at all computational tasks. Multiplication for example, will not be performed any quicker on a quantum computer than it could be done on a similar classical computer. In order for a quantum computer to show its superiority it needs to use algorithms that exploit its power of quantum parallelism. Such algorithms are difficult to formulate, to date the most significant theorized being Shor's algorithm and Grover's algorithm. By using these algorithms a quantum computer will be able to outperform classical computers by a significant margin. For example, Shor's algorithm allows extremely quick factoring of large numbers, a classical computer can be estimated at taking 10 million billion billion years to factor a 1000 digit number, where as a quantum computer would take around 20 minutes.

12.1 Quantum communication

The research carried out on quantum computing has created the spin-off field of quantum communication. This area of research aims to provide secure communication mechanisms by using the properties of quantum mechanical effects.

12.2 How quantum communication works

Quantum communications makes use of the fact that information can be encoded as the polarisation of photons (i.e. the orientation of a photon's oscillation). An oscillation in one direction can be thought of as 0 and in another as a 1. The polarisation of photons can be used to encode data. In order to receive the data, the polarization of the filter must match that of the photons.

The property that quantum communication exploits is that in order to receive the correct information, photons have to be measured using the correct filter polarisation e.g. the same polarisation that the information was transmitted with. If a receiver is in rectilinear polarisation, and a diagonally polarised photon is sent, then a completely random result will appear at the receiver. Using this, property information can be sent in such a way as to make it impossible for an eavesdropper to listen undetected. The mechanism by which this works is as follows:

1. The sender transmits information to the receiver using random polarisations.
2. The receiver detects this information (also at random polarisations) and records it.
3. The sender informs the receiver of the polarisations that he used over a public channel.
4. The receiver and sender compare a random selection of the information that was received at the correct polarisation.
5. If an eavesdropper has intercepted and forwarded the information, the receiver and sender will be alerted as a higher percentage of errors will be present than expected.
6. If an eavesdropper has been detected, then the whole process has to be repeated.

British Telecom has managed to implement a line with only 9% error over a distance of 10km, giving quantum communications a promising future.

12.3 Current progress & future prospects

The recent work on the 'computing liquid' technique pioneered by Dr. Gershenfield and Dr. Chuang (Los Alamos National Laboratory, New Mexico) has given quantum computing a promising future. In fact, Dr. Gershenfield believes that a quantum co-processor could be a reality within 10 years if the current pace of advancement continues. Other techniques, such as quantum dots, may also yield similar results as our technology advances. The optimist will point out that the problems being experienced by researchers appear to be technical rather than fundamental. On the other side of the argument, is the topic of decoherence. This problem has not been resolved and many people, including Rolf Landauer of IBM's Thomas Watson Research Centre, believe that the quantum computer is unlikely to progress beyond the 10-qubit system (described above), as decoherence makes them too fragile to be practical.

Error correction has made promising progress to date, nearing a point now where we may have the tools required to build a computer robust enough to adequately withstand the effects of decoherence. Quantum hardware, on the other hand, remains an emerging field, but the work done thus far suggests that it will only be a matter time before we have devices large enough to test Shor's and other quantum algorithms. Quantum computation has its origins in highly specialized fields of theoretical physics, but its future undoubtedly lies in the profound effect it will have on the lives of all mankind.

13. FUTURE BENEFITS OF QUANTUM COMPUTERS

13.1 Cryptography and Peter Shor’s Algorithm

In 1994 Peter Shor (Bell Laboratories) found out the first quantum algorithm that, in principle, can perform an efficient factorization. This became a complex application that only a quantum computer could do. Factoring is one of the most important problems in cryptography. For instance, the security of RSA (electronic banking security system) - public key cryptography - depends on factoring and it is a big problem. Because of many useful features of quantum computer, scientists put more efforts to build it. However, breaking any kind of current encryption that takes almost centuries on existing computers, may just take a few years on quantum computer. (Maney, 1998)

13.2 Artificial Intelligence

It has been mentioned that quantum computers will be much faster and consequently will perform a large amount of operations in a very short period of time. On the other side, increasing the speed of operation will help computers to learn faster even using the one of the simplest methods - mistake bound model for learning.

13.3 Other Benefits

High performance will allow us in development of complex compression algorithms, voice and image recognition, molecular simulations, true randomness and quantum communication. Randomness is important in simulations. Molecular simulations are important for developing simulation applications for chemistry and biology. With the help of quantum communication both receiver and sender are alerted when an eavesdropper tries to catch the signal. Quantum bits also allow more information to be communicated per bit. Quantum computers make communication more secure.

14. CONCLUSION

The quantum computers power to perform calculations across a multitude of parallel universes gives it the ability to quickly perform tasks that classical computers will never be able to practically achieve. This power can only be unleashed with the correct type of algorithm, a type of algorithm that is extremely difficult to formulate. Some algorithms have already been invented; they are proving to have huge implications on the world of cryptography. This is because they enable the most commonly used cryptography techniques to be broken in a matter of seconds. Ironically, a spin-off of quantum computing, quantum communication allows information to be sent without eavesdroppers listening undetected.

For now at least, the world of cryptography is safe because the quantum computer is proving to be very difficult to implement. The very thing that makes them powerful, their reliance on quantum mechanics, also makes them extremely fragile. The most successful experiments only being able to add one and one together. Nobody can tell if the problems being experienced by researchers can be overcome, some like Dr. Gershenfield are hopeful that they can whilst others believe that the quantum computer will always be too fragile to be practical.

It is important that making a practical quantum computing is still far in the future. Programming style for a quantum computer will also be quite different. Development of quantum computer needs a lot of money. Even the best scientists can’t answer a lot of questions about quantum physics. Quantum computer is based on theoretical physics and some experiments are already made. Building a practical quantum computer is just a matter of time. Quantum computers easily solve applications that can’t be done with help of today’s computers. This will be one of the biggest steps in science and will undoubtedly revolutionize the practical computing world.

REFERENCES:

1. The Fabric of Reality. David Deutsch
2. Physics - A Textbook for Advanced Level Students. Tom Duncan
   A brief introduction to elementary quantum physics
3. Algorithmics - The Spirit of Computing. David Harel
4. A quantum revolution for computing. Julian Brown, New Scientist 24/9/94
5. The best computer in all possible worlds. Tim Folger, Discover 1/10/95
6. Cue the qubits: Quantum computing - How to make a quantum computer.
7. Quantum keys for keeping secrets. Artur Ekert, New Scientist Volume 137
8. Bulk Spin Resonance Quantum Computation http://feynman.stanford.edu