A Brief Study on Quantum Computing

Preeta Chatterjee[1], Rishika Chakraborty[1]

[1]Department of Electronics and Communication Engineering, Institute of Engineering and Management, Kolkata-700091

Email: c.preeta6@gmail.com

Abstract

In the twentieth century, quantum physics is one of the most successful approaches in scientific progress. To theorize the concept of quantum computing Max Planck's idea of the existence of energy in individual units like matter was used. Since then, the idea of manufacturing quantum computers for everyday use is becoming more plausible with technological advances in quantum theory. A classical computer carries out logical operations using a bit which is either 1 or 0. In contrast to a classical computer, a quantum computer works with a quantum bit or qubit, which is not limited to two states only. Qubits can exist in a superposition of the two states creating parallelism. Qubit represents the state of atoms, ions, photons or electrons. These qubits which work together with a control device act as a computer memory.

Quantum computers have the potential to become million times more potent than present-day supercomputers due to the presence of these multiple states simultaneously. Concepts and ideas of quantum computing have been demonstrated by different methods like Ion Trap, Quantum Dot methods etc. However, the actual realization of such a superior system is still in the future. A strategy must be formulated to maintain decoherence and other potential sources of error at a permissible level.

Astonishingly, quantum computing took a long time to take off, even though the physicists have known about the world of subatomic particles. Even so, it took computer scientists another half-century to consider harnessing quantum effects for computation. Also, it was later discovered that quantum computers could solve quantum mechanical many-body problems that are impractical to solve on a classical computer. The foundations of the subject of quantum computation may have become well-published, but the knowledge is still growing. Hence here is a research paper based on the study of quantum computation.

Keywords: *Quantum Theory, Quantum Computing, Qubits, Parallelism, Ion Trap method, Quantum Dot Method.*

1. Introduction

With the development of science and technology, new ways were discovered for the exploitation of various physical resources such as materials, forces and energies. This gradually leads to the advancement of civilizations as a whole. The history of computer development represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage and the eventual creation of the first computer, followed by Alan Turing's ground-breaking work in computing and Artificial Intelligence and the decoding of the German Enigma code. The process involved is a sequence of changes from one type of physical realization to another, from gears to valves to transistors to integrated circuits to chips and so on.

Nowadays, although computers have become more compact and considerably faster, their tasks remain the same: to manipulate and interpret an encoding binary bit into a useful computational result.

Matter obeys the rules of quantum mechanics, which are quite different from classical rules that determine the properties of conventional logic gates. If computers are to become smaller, then quantum technology must replace what we have now, since it can offer new types of computation both quantitatively and qualitatively and provide new algorithms based on the principles of quantum mechanics. Due to the physical limitations of the classical computer and the ability of quantum computers to perform those specific tasks more rapidly than a classical computer, the study of quantum computation is required. Concepts of quantum mechanics are applied to make quantum computers a possibility.

2. Evolution of Quantum Computing

In the 1970s and the early 1980s**,** the idea of computational devices based on quantum mechanics was first explored by physicists and computer scientists Charles H. Bennet, Paul A. Benioff, David Deutsch and Richard P. Feynman. The concept emerged once scientists were musing over basic limits of computation. The scientists steered in this system that experiments may well be carried out in quantum physics inside a quantum mechanical computer. To solve a solve quantum mechanical many-body problems on a classical computer it requires exponentially growing time. In contrast to this, the whole calculations on the quantum computer can be done in polynomial time. In 1994, a method was invented by Peter Shor to solve an infamous problem in number theory, namely, factorization, with the help of quantum computers. It was shown that an ensemble of mathematical operations, explicitly designed for a quantum computer could be organized to make such a machine to factor huge numbers within a short time and the computational time is orders of magnitude smaller than that on conventional computers. This advancement of quantum computing embarked on the path of interest of all researchers in the world.

3. Limitations of Classical Computers

3.1 Public Key Cryptography and Classical Factoring of Big Integers

A creative mathematical discovery In 1970s in the shape of the "Public Key" systems provided a solution to the key distribution problem. In these kinds of scenarios, users do not need to agree on a secret key before sending a message. The principle of a safe with two keys is employed, where one public access is used to lock it, and the other private key is used to open it. These two keys are in practice large integer numbers. One can easily derive the public key from the private key but not vice-versa. This fact behind the process is that some mathematical operations are more accessible to perform in one direction than the other. For example, multiplication of two numbers can be performed a lot more quickly than factorizing the numbers. An algorithm can be defined as a fast algorithm if the time taken to complete the algorithm does not increase too sharply when the same process is applied to large numbers. For example, multiplication of two thirty-digit numbers by trial division method takes up a lot more time than that of two three-digit numbers. Hence the trial division method is not a fast algorithm in all cases. It is seen that public key cryptosystems could avoid the fundamental distribution problem. However, the security depends upon unproven mathematical assumptions such as the difficulty of factoring large integers.

3.2 Quantum Factoring

Factorization of huge numbers is beyond the capabilities of any computing devices unless the computer scientists or the mathematicians create an efficient factoring algorithm. The public key cryptosystems will remain secure. However, it turns out that it is not the case. The Classical Theory of Computation cannot describe all possible computation. There it is not a complete theory of computation. The analyses which can be performed by quantum devices cannot be described by Classical Theory of Computation. A quantum computer can factor much faster than any classical computer has been already described in some recent papers. Peter Shor developed an algorithm which gives the factoring of an integer on quantum computers runs in $O\left((\ln N)^{(2+\epsilon)}\right)$ steps, where ϵ is small. Since this is quadratic in the input size, factoring a 1000-digit number with such an algorithm requires a few million steps. The inference obtained from this is that the public key cryptosystems based on factoring may be breakable.

3.3 Searching of an Item with Desired Property

Quantum logic-based algorithm can search an item with the desired property from a collection of N items with a competitive speed. For example, from a group of N items, a random item is picked up. The likelihood of correct selection is the same as that of the right one—this probability of the right choice in half. Hence on average N/2 operations are required for getting the correct item where the quantum logic-based algorithm by Grover completes the same task in an average of $N^{\frac{1}{2}}$ number of operations.

4. Birth of Art of Quantum Computing

Richard P. Feynman in 1982, proposed that the usual computer cannot simulate a quantum physical system of N particles with its quantum probabilities without an exponential slowdown in the efficiency of the simulation. However, in classical physics, they can be simulated with a polynomial slowdown. The main reason is that the description size of a particle system, user without an exponential slowdown in the efficiency of the simulation. However, in classical physics, they can be simulated with a polynomial slowdown. The main reason is that the description size of the particle system is linear in N in classical physics but exponential in N in a quantum computer. This can help to avoid the slowdown encountered in the simulation of quantum systems. Feynman also addressed that the problem of simulating a quantum physical system with a probabilistic computer is due to the interference phenomena. Thus, all these factors stimulated the birth of quantum computing to allow the usage of quantum computers, overcoming all the limitations of classical computers.

5. Quantum Computing – Parallelism

Classical computers operate by dividing a task into elementary operations to be carried out serially, one operation at a time. Attempts have been made at making two computers work simultaneously to approach different aspects of a problem at the same time, but these have not been very successful. The major reason for this is the logic built into the microprocessors used is inherently serial as even during the times when a classical computer appears to be doing several tasks at once, it just cycles between the steps rapidly one at a time. This is the reason why solving complex, and massive problems put constraints on even the fastest supercomputers. These computers are inefficient for these tasks, not that their microprocessors are slow.

A computer should have parallelism built into it to face a problem with simultaneity. Such computers exist and are called Quantum Computers. The principle of linear superposition tells that the quantum system in a quantum state consists of a superposition of many classical and classical-like states. If this superposition can be protected from all other outwardly interferences from the environment, then a quantum computer can give results depending on all its different classical states. This is quantum parallelism.

6. Concepts of Quantum Computers

Contrary to classical computers, the fundamental unit of information in a quantum computer is not binary but more quaternary in nature. It is called a "qubit" (short for a quantum bit), and it is analogous to "bit" used in classical computers. The properties of qubit come from its adherence to laws of quantum mechanics. We can place a qubit not only in the logical state 0 or 1 but in both 0 and 1 simultaneously, with a numerical coefficient which represents the probability for each state. This makes the concept seem dubious since quantum mechanics works only at the atomic level, and Classical Mechanics, govern real-life situations.

Physically, the qubit can be visualized as the spin of a one-electron system (s=1/2); the two-state +1/2 and -1/2 are the eigenstates of the z - component of an external magnetic field of spin ½. Thus, the qubit can take two values, 0 or 1, associated with these two eigenstates of a spin of a single electron.

It can also be the superposition of these two states with complex coefficients. This is the property which distinguishes qubits from classical bits used in conventional computers.

7. Experimental Realization of Quantum Computing

Architecturally, the simplistic model of quantum computers makes it faster, cheaper and smaller. However, the conceptual intricacies in its making its experimental realization extremely difficult, and for a time, unrealistic. Nevertheless, there have been a lot of attempts in this direction with some encouraging results. Maybe quantum computers replacing classical computers is not very far off reality.
Some of such attempts are listed below:

7.1 Heteropolymer based Quantum Computers

In 1988 the first heteropolymer based quantum computer was designed and built-in by Teich and later improved by Lloyd in 1993. A linear array of atoms is used as memory cells in this heteropolymer based quantum computer. By pumping the corresponding atom into an excited state information is stored on a cell. The transmission of the instruction to the heteropolymer is happened by laser pulses of appropriately tuned frequencies. The nature of the computation that is performed on selected atoms is determined by the shape and the duration of the pulse.

7.2 Ion Trap Quantum Computers

Cirac and Zoller In the year of 1995 first proposed an ion trapped in an external potential can be used as qubits in a quantum computer. It was implemented first by Monroe and collaborators in 1995 and then by Schwarzchild in 1996. The data is encoded in the energy states of ions and the vibrational modes between

the ions in an ion trap computer. In theory, a separate laser operates each ion. Evaluation of Fourier transforms with the ion trap computer was found feasible on preliminary tests.

7.3 Quantum Electrodynamics Cavity Computers

In the year of 1995, quantum electrodynamics (QED) cavity computer was demonstrated by Turchetta and collaborators which consists of a QED cavity filled with some Caesium atoms and an arrangement of lasers, phase shift detectors, polarizer and mirrors. The computer gave the real model of a quantum computer which can create, manipulate and preserve superposition and entanglements.

7.4 Quantum Dot Technology

Quantum dots are semiconductor nanostructures having a size less than or equal to its exciton-Bohr radius. The quantum dots have the typical size between $\sim 10\ nm$ and $\sim 100\ nm$. Among various types of quantum dots, the electrostatic quantum dots are best candidates for the implementation of quantum logic gates. An array of quantum dots, in which the dots are connected with their nearest neighbours through gated tunnelling barriers, for fabricating quantum gates using the split-gate technique.

8. Conclusion

Quantum computation has become a well-established subject of interest, but opportunities for its future growth are still being pursued. The study is ongoing in quantum algorithms, logic gate operations, error correction, understanding dynamics and control of decoherence, atomic-scale technology and practical applications. New algorithms can be found with the help of the properties of complex numbers (analytic functions, conformal mappings). Required theoretical tools for solving many-body quantum entanglement, are not well developed. Its improved characterization can do the better implementation of quantum logic gates and correction of correlated errors.

Quantum building blocks are the constituents of the system and the observer, yet neither the decoherence nor the measurement has been understood fully yet. The transition from classical to the quantum regime is fascinating to study. If there is something beyond quantum theory, it would be noticed in the struggle for making quantum devices. New limitations of quantum theory may be discovered while trying to conquer decoherence.

The race for miniaturization of electronic circuits is not too far away from the quantum reality of nature. The new paradigm of quantum computing will accelerate AI development and help us develop the innovations of tomorrow. Leading AI companies are making advances in quantum computing by developing quantum processors and novel quantum algorithms.

9. Acknowledgements

We sincerely acknowledge Ms Prajna Paromita Chanda for her constant help.

REFERENCES

[1] Nielsen, M. E., Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information*. (Cambridge University Press, 2000).

[2] Kloeffel, C. & Loss, D. Prospects for Spin-Based Quantum Computing in Quantum Dots. *Annu. Rev. Condens. Matter Phys.* **4,** 51–81 (2013).

[3] Prashant. A Study on the basics of Quantum Computing. *arXiv:quant-ph/0511061.*

[4] Mendonca, J. T. *Theory of Photon Acceleration*. (CRC Press, 2000).

[5] Duncan, T. *Physics: A Textbook for Advanced Level Students*. (Coronet Books, 1982).