International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 02 | Feb-2018 www.irjet.net p-ISSN: 2395-0072

AN OVERVIEW OF QUANTUM COMPUTING

Arockia Panimalar.S[1], Nishanth.R[2], Abin Henry[3], Monica.J[4]

[1]Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu
[2,3,4] III BCA A, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu

---

Abstract: *Transmutating the model, its underlying information and computation from classic mechanical to quantum mechanical, one yields faster algorithms, novel cryptographic and alternative methods of communication. The depth of quantum computing applications is still being explored. Quantum algorithm could perform a set of work more differently and efficiently than other classical algorithms, but for some tasks, it is been proved that the quantum algorithms don't provide any advantage. Major application areas include security and the many fields that would benefit from an efficient quantum simulation. Details of the quantum viewpoints provide awareness in classical algorithm problems and as well as a deeper understanding and other non-classical details of quantum physics.*

Key Words: *Quantum Computing, Cryptography, Qubits, Entanglement, Public Key Cryptography*.

1. INTRODUCTION

Now-a-days many computers don't have any transistors and chips. If a computer that is faster than common classical silicon computer it is called as a quantum computer. Clearly, it can run without consuming more energy and million times faster than today's Pentium III computers. Scientists think that a quantum computer will be the next generation of classical computers.

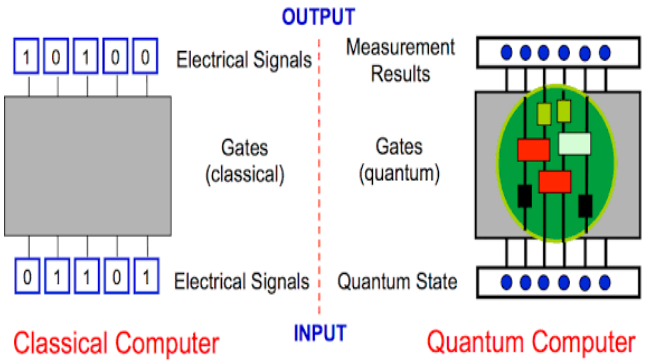
Gershenfeld says that if making of transistors smaller and smaller is continued with the same rate as in the past years, then by the year of 2020, the width of a wire in a computer chip will be no more than a size of a single atom. These are sizes for which rule of classical physics no longer apply. Computers designed on today's chip technology will not continue to get cheaper and better. Because of its great power, a quantum computer is an attractive next step in computer technology. A technology of quantum computers is also very different. Qubit have a quaternary nature. Quantum mechanics laws are completely different from the laws of a classical physics. A qubit will be in existence not only in the states corresponding to the logical values of 0 or 1 but in the case of a classical bit and also in a superposition state.

A qubit is a bit of information that can be both zero's and one's simultaneously (superposition state). Therefore a computer working on a qubit than a standard bit can make calculations using both values. A qubyte is made up of eight qubit and can have all the values from 0 to 255. Forty qubits could have the same power as modern supercomputers. 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 the development of the quantum computer.

2. THE MAJOR DIFFERENCE BETWEEN QUANTUM AND CLASSICAL COMPUTERS

A classical computer has a string value of 0 and 1, and it will perform calculations on one set of numbers at a time. The memory of a quantum computer is in a quantum state that can be of different numbers. A quantum computer can do an arbitrary reverse classical computation on all the numbers. Performing a computation on different numbers at a time and then interrupting all the results to get a single answer, makes a quantum computer more powerful than a normal one.



3. BASIC CONCEPTS OF QUANTUM COMPUTATION

The state space of a physical system consists of all possible states of the system. Any quantum mechanical system that can be modeled by a two dimensional complex vector space can be viewed as a qubit. Such systems include photon polarization, electron spin, and a ground state and an excited state of an atom. A key difference between classical and quantum systems is the way in which component systems combine. The state of a classical system can be completely characterized by the state of each of its component pieces. A surprising and unintuitive aspect of quantum systems is that, most states cannot be described in terms of the states of the system's components. Such states are called entangled states. Another key property is quantum measurement.

In spite of there being a continuum of possible states, any measurement of a system of qubits has only a discrete set of possible outcomes for n qubits, there are at most 2n possible outcomes. After measurement, the system will be in one of the possible outcome states. Which outcome is obtained is probabilistic, outcomes closest to the measured state are most probable. Unless the state is already in one of the possible outcome states, measurement changes the state, it is not possible to reliably measure an unknown state without disturbing it. Similarly as every estimation has a discrete arrangement of possible outcomes, any mechanism for replicating quantum states can just accurately copy a discrete arrangement of quantum states. For a n qubit system, the biggest number of quantum states a copying mechanism can copy correctly is 2n. For any state there is a mechanism that can correctly copy it, but if the state is unknown, there is no way to determine which mechanism should be used. For this reason, it is impossible to copy reliably an unknown state, an aspect of quantum mechanics called the no cloning principle.

A qubit has two arbitrarily chosen distinguished states, labeled as |0i and |1i, which are the possible outcomes of a single measurement. Every single qubit state can be represented as a linear combination, or superposition of these two states. In quantum information processing, classical bit values of 0 and 1 are encoded in the distinguished states |0i and |1i. This encoding enables a direct comparison between bits and qubits. Bits can only take on two values 0 and 1, while qubits can take on any superposition of these values, a|0i+b|1i, where a and b are complex numbers such that |a|2+|b|2=1. Any transformation of an n qubit system can be obtained by performing a sequence of one and two qubit operations.

4. FUTURE BENEFITS OF QUANTUM COMPUTERS

4.1 Cryptography and Peter Shor's Algorithm

In 1994 Peter Shor found that the first quantum algorithm in principle can perform more efficient factorization in bell laboratories. This has become a complex application that only a quantum computer will do efficiently. Factoring is one of the most important problems in cryptography. For instance, the security of RSA- a public key cryptography depends on factoring and it is a big problem. Because of many useful features of the quantum computer, scientists put more efforts to build it. In any case, breaking any sort of current encryption that takes nearly hundreds of years on existing PCs may simply take a couple of years on the quantum PC.

4.2 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 one of the simplest methods naming mistake bound model.

4.3 Other Benefits

Development of complex compression algorithms, voice and image recognition, molecular simulations, true randomness and quantum communication can be done with high performance. In simulations, randomness is more important. Molecular simulations are more important for the development of simulation applications in chemistry as well as 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.

5. LIMITATIONS OF QUANTUM COMPUTING

Beals et al. proved that, for a broad class of problems, quantum computation cannot provide any speed-up. Their methods were used by others to provide lower bounds for other types of problems. Ambainis found another powerful method for establishing lower bounds. In 2002, Aaronson demonstrated that quantum methodologies couldn't be utilized to proficiently take care of collision issues. This implies there is no bland quantum attack on cryptographic hash functions. Shor's calculations break some cryptographic hash functions and quantum attacks on others may in any case be found, yet Aaronson's outcome says that any attack must utilize particular properties of the hash work under thought. Grover's pursuit calculation is ideal. It is not possible to search an unstructured list of N elements more rapidly than $O(\sqrt{N})$. This bound was known before Grover found his algorithm. Childs et al. showed that for ordered data, quantum computation can give no more that a constant factor improvement over optimal classical algorithms. Grigni et al. showed in 2001 that for most non-abelian groups and their subgroups, the standard Fourier sampling method, used by Shor and successors, yields exponentially little information about a hidden subgroup.

6. ENTANGLEMENT OF QUANTUM SYSTEMS

According to quantum mechanics, an outside force acting on two particles of the quantum system can cause them to become entangled. The quantum state of this system contains all positions of spins (internal magnetic moments) of each particle. The total spin of the system can only be equal to certain discrete values with different probabilities. Measurements of total spin of certain quantum systems showed that positions of spins of some particle are not independent from others. For such systems, when an orientation of a spin of one particle changed by some reason, an orientation of a spin of another particle changes automatically and instantly. The laws that that have been developed so far about the speed of light are disobeyed in this case, because the change in an orientation of a spin

happens immediately. At least there is hypothesizing to use this phenomenon for quantum computing.

It is well known that a speed of communication is limited by a speed of light as nothing can travel faster than the speed of light. The question is how particles of the quantum system communicate when they change their spin orientation and consequently their vector states. Famous scientists spent a lot of time discussing this issue. Einstein's idea that some unknown "hidden parameters" of quantum system were contributing to this effect has been rejected theoretically and experimentally. This is one of the example showing the difference between classical and quantum realities. This effect of the quantum system explains a lot of aspects of the nature (i.e. chemical characteristics of atoms and molecules) and is proved by the experiments.

Infact, theories about entanglement have led scientists to believe there could be a way to speed up computing. Even today's computers are nearing a point at which their speed is being limited by how fast an electron can move through a wire - the speed of light. Whether in a quantum or traditional computer, entanglement could blow past that limit.

7. CONCLUSION

Computing of practical quantum is important in the future. Programming a style for the quantum computer will also be different. A lot of money is needed for the development of the quantum computer. Even the most experienced and well-scholared scientists can't answer a lot of questions about quantum physics. Quantum computers are based on theoretical physics and some experiments that are made. Building of a practical quantum computer takes a little bit time. Applications that can't be done with help of today's computers can be easily done with the help of quantum computers. This could be one of the most revolutionary way in the practical computer world and it is a giant leap for mankind in the era of computers

8. REFERENCES

[1] Daniel, G. (1999). "Quantum Error Correcting Codes", from: http://qso.lanl.gov/gottesma/QECC.html

[2] Manay, K. (1998). "Quantum computers could be a billion times faster than Pentium III", USA Today, Dec, 2002 from:http://www.amd1.com/quantum_computers.html

[3] S. Aaronson. "The limits of quantum computers", Scientific American, 298(3):62 – 69, Mar. 2008.

[4] Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev. Adiabatic quantum computation is equivalent to standard quantum computation. SIAM Journal on Computing, 37:166, 2007.

[5] H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. Scientific American, 267(4):50, Oct. 1992.

[6] C. M. Carollo and V. Vedral. Holonomic quantum computation. arXiv:quant-ph/0504205, 2005

[7] R.Feynman. Feynman Lectures on Computation. Addison Wesley, Reading, MA, 1996.