International Journal of Engineering Innovation & Research
Volume 1, Issue 2, ISSN : 2277 – 5668

Study of Quantum Computing

Kanchan Vishalkumar Wankhade
dangekanchan05@gmail.com

Prashant Anil Patil
patilpait@gmail.com

Seema Nathu Lokhande
seemanlokhande@gmail.com

***Abstract* — This paper gives the detailed information about Quantum computer, and difference between quantum computer and traditional computers, the basis of Quantum computers which are slightly similar but still different from traditional computer. Many research groups are working towards the highly technological goal of building a quantum computer, which would dramatically improve computational power for particular tasks. Quantum computer is very much use full for computation purpose in field of Science and Research. Large amount of data and information will be computed, processing, storing, retrieving, transmitting and displaying information in less time with that much of accuracy which is not provided by traditional computers.**

***Key Words* — Qubits, Turing machine, RSA algorithm, Brute Force approach, Quantum Computing.**

I. INTRODUCTION

Quantum computing is the term used to solve problems much faster and efficient way than any traditional computer using presently available algorithms. It uses entanglement and superposition i.e. the quantum mechanical phenomenon for performing operations on data. The basic rule behind quantum computation is quantum properties are able to represent data and can perform operations on these data[8]. In classical computer, the basic building block is bit, it can exist in one of two states, a 0 or a 1. In a quantum computer a quantum bit, referred to as a qubit can exist in the 0 and 1 states also it can be in a coherent superposition of both. When a qubit is in this state it can be thought of as existing in two universes[11].

An operation on a qubit in this state is performed on both the values. Quantum computing is very sensitive & difficult to control. As soon as qubit in coherent state interacts with the environment it will decohere and fall into one of the two states 0 or 1. Operations on this bit have results in both the universe & a measurable result is calculated using them.

Computers are implementations of a universal Turing machine. They are all equivalent functionally and still some are quicker, larger or some are expensive. All perform the same set of computational tasks. Inputs can be easily guessed from the output i.e.no information is lost [11].

II. BUILDIG UP A QUANTUM COMPUER

A. Quantum dots

One of the implementation of the qubit is the quantum dot. It is single electron inside a group of atoms. When the dot is exposed to a pulse of laser light of appropriate wavelength and duration, the electron is raised to an excited state & in the second burst of laser causes the electron to fall back to its ground state. The ground state and excited states can be considered as the 0 and 1 states of the qubit. 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 it goes to the coherent state of the qubit. More complex logic functions can be modelled using quantum dots arranged in pairs [11].

B. Computing liquids

Uses a collection of molecules to store the information. Each nucleus within a molecule spins in a certain direction, when held in a magnetic field & it can describe its state (spinning upwards 1, spinning down 0). Nuclear Magnetic Resonance (NMR) techniques can be useful to detect the spins states. It instead uses a whole set of liquid molecules. Even though collisions arise the spin states of the nuclei within remain unchanged but decoherence is still a problem. Dr. Gershenfield from the Massachusetts Institute of Technology is one of the pioneers of the computing liquid technique. Addition of one and one is possible by his team. More complex tasks would need more qubits but this requires more complex molecules with a greater number of nuclei [11].

A system with more than10 qubits is 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. There is a limit on the number of qubits a system may have as the readable output will be harder to detect.

III. NEED OF QUANTUM COMPUTING

Though there are many technologies that enhanced the processing capability of computers but our expectations were increasing. Furthermore, the significant increase in the use of personal computers and internet boosted the processing power. Still our desire for more memory and computing power was not fulfilled so, new technology to overcome this is Quantum computing which is having power of atoms and molecules to perform and represent data. Quantum computing was first introduced by Paul Benioff in 1982 [12].

The Traditional computers works on binary bits i.e., either one or zero. But, the Quantum computers are not stick to the binary approach they observe the state of quantum bit or qubits which might be zero or one or a combination of two or superposition of both means state of qubit somewhere between 1 and 0. The quantum parallelism is main force behind development of quantum computing which states that a processor that uses registers of qubits will be able to perform operations on all possible values of the input registers simultaneously [1].

IV. Advantages And Disadvantages

There are various models for quantum computing are introduced and their advantages as well as disadvantages are described. The *advantages* are as follows:

i. It can outperform traditional computers using new algorithms in an efficient manner [13].
ii. As quantum computing have ability to break codes so, can be used to protect transactions over the internet [2].
iii. Hard problems are quickly get solved like prime number factorization problem [4].
iv. It can easily simulate protein folding [5].
v. It can easily manipulate the set of linear equations with wave nature [5].

The *disadvantages* associated with quantum computing are:

i. Information can be lost as electron only remains in excited state for about a microsecond [13].
ii. The technology to build a computer from quantum dots doesn't yet exist.
iii. It requires new algorithms to implement quantum computing so, it is not so easy to formulate such algorithms [13].
iv. Lasers can cram in tiny spaces so quantum dots must respond to different frequencies.

V. Applications

A. *Searching of data*

A quantum computer takes in general square root (y) steps. Quantum search algorithms can be much faster to search data among the extensively large amount of data. It applies brute force approach to search data & does it until it finds solution [7].

B. *Security*

Quantum computation can help in factoring the two integers which can easily reveal the keys used in public key cryptography. For example in RSA algorithm public key which is used for encryption can easily be computed using the private key, but it can be done much more faster using quantum approach & can break the keys by factorizing in small time; which will take millions of years for classical computers [11].

C. *Applications in data analysis*

Scientific calculations for weather forecasting, financial analysis & higher mathematical calculations
can be done using quantum computations [6].

VI. Challenges

1) There is problem regarding coupling of qubits, if qubit A needs to be coupled with qubit B for changing the state of qubit B. So, for this we constantly need to keep link active. But, active link may result change in state of qubit A [14].
2) Qubits are not easy to handle for doing something useful. Qubits are extremely fragile and decohere also can possibly leak information into environment. There is need of qubits those are poked and can survive for long time period [10].
3) Impurities into solid-state devices can cause limit for use of quantum computing. The biggest challenge is how to use solid-state devices without actually concerning with their physical characteristics [3].

Conclusion

We have done the case study for Quantum computing and come to a conclusion that we can increase computational power using qubits which was not provided by Traditional computers.

Quantum computers have ability to perform quickly which cannot be practically achieved by Traditional computers. But, this ability only comes with correct type of algorithm.

The World of cryptography is now safe as quantum computers provides unbreakable ciphers and soon will allow cracking of every single cipher.

References

[1] IEEE Bombay, "Quantum Computers" , IEEE Journal [Online], Available:http://ewh.ieee.org/r10/bombay/news4/Quantum_Computers.htm
[2] Scott Aaronson & Dave Bacon (2008, Dec 12). "Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment", (6th ed.) [Online]. Available: www.cra.org/ccc/docs/init/Quantum_Computing.pdf
[3] Keyes R.W., (2005, Jan), "Challenges for quantum computing with solid-state devices", IEEE Computer Society[Online], *38(1).* pp. 65-69. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1381257
[4] Lov K. Grover (1998, Apr 10), "QUANTUM COMPUTING: The Advantages of Superposition", Science Magazine[Online], 280(5361), pp. 228. Available: http://www.sciencemag.org/content/280/5361/228
[5] NOVA(2011, Jul 7), "A Quantum Leap in Computing", Tech+ Engineering[Online], Available: http://www.pbs.org/wgbh/nova/tech/quantum-computing.html
[6] Larry Hardesty(2009, Oct 9), "Quantum computing may actually be useful", MIT News Office[Online], Available: web.mit.edu/newsoffice/2009/quantum-algorithm.html
[7] Richard Murch(2005, Mar 18), "Quantum Computing: The Hype and Reality", IBM Press[Online], Available: http://www.ibmpressbooks.com/articles/article.asp?p=374693&seqNum=5
[8] Wikipedia, "Quantum computer", Available: http://en.wikipedia.org/wiki/Quantum_computer
[9] Carolla Development, "Quantum Computers: What are They and What Do They Mean to Us?", Available: www.carolla.com/quantum/QuantumComputers.htm
[10] KFC(2009, May 04), "Diamond Challenges for Quantum-Computing Crown", Physics arXiv Blog[Online], Available: http://www.technologyreview.in/blog/arxiv/23479/
[11] Simon Bone and Matias Castro(1997, May), "A Brief History of Quantum Computing", Available: http://www.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/
[12] Kevin Bonsor and Jonathan Strickland, "How Quantum Computers Work", Tech[Online], Available: http://computer.howstuffworks.com/quantum-computer.htm
[13] Shivam agrawal, "Advantages and disadvantages of quantum computers?" wiki answers[Online], Available: http://wiki.answers.com/Q/Advantages_and_disadvantages_of_quantum_computers

[14] Cyrus Farivar(2007, Jul 05), “It's the "Wiring" That's Tricky in Quantum Computing”, WIRED Magazine[Online], Available: http://www.wired.com/science/discoveries/news/2007/05/quantumcoupling

AUTHOUR’S PROFILE

Mrs. Kanchan V. Wankhade, she is presently Lecturer in Information Technology Department, in Dhole Patil College of Engineering Wagholi ,Pune. She has completed Bachelors Degree in Information Technology and PGD-C-DAC.

Prashant A. Patil, he is currently pursuing his B.E. (I.T.) from Dhole Patil Collegge of Engg. , Wagholi, Pune. He is working regarding his project Network Monitoring System on which he has already published paper in IJECCE-2011.

Seema N. Lokhande, she is currently pursuing her B.E.(I.T.) from Dhole Patil Collegge of Engg. , Wagholi, Pune. She is working regarding her project Network Monitoring System on which she has already published paper in IJECCE-2011 along with her colleague Prashant A. Patil