International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
69 – 71

An Insight into Quantum Computers

Anubha Datey
Dept. of Computer Science and Engineering
Raipur, Chhattisgarh
anubhadatey@gmail.com

Anisha Sharma
Dept. of Computer Science and Engineering
Raipur, Chhattisgarh
Anishasharma65@gmail.com

***Abstract*—** This paper provides the central idea of quantum computers and many other essential aspects. A reader needs no prior knowledge to know the essentials of Quantum Computer. This paper will thus allow newcomers to obtain a broad overview of the important techniques and results of this field.

***Index Terms*—** *Quantum Computer, Classical Computer, Quantum Bit (Qubit), Quantum Register, Quantum Computing, Classical Computing, Shor's Algorithm, Grover's Algorithm, Boson's Algorithm, Superposition, Entanglement.*

*****

I. INTRODUCTION

Quantum Computing is an emerging field of study. In 1965, physicist Gordon Moore predicted that the number of transistors in a chip would double in every 18 months, so the size of transistors must shrink exponentially. Now we are approaching the physical limits of Moore's law, below that, is the frontier of the quantum scale where wave particle duality can be used to our advantage. Therefore scientists are developing quantum computers which illuminate the basic ideas of quantum mechanics. Quantum computer encodes information in quantum particles. It manipulates them and then does the computation. [1]

A. Quantum Bits and Quantum Registers

Classical computer uses bits which are either 0 or 1 but quantum computers uses quantum bits (Qubits) which can be both 0 and 1 simultaneously, thus providing larger possibility of states that you can explore. There are number of physical objects that can be used as a qubit, such as a single photon, a nucleus or an electron.

Like classical computers, quantum computer uses quantum register, which is a combination of multiple qubits for performing computation. When collapsed, quantum registers are bit strings, whose length determines the amount of information they store.

B. Superposition

One of the distinguishing characteristic of quantum computer is Superposition or to be specific superposition principle of quantum mechanics. Rather than being in one of the possible states at a time, a quantum system can exist in combination of all possible particle states simultaneously. But when the quantum system is measured, it collapses into an observable, definite classical state. This characteristic of quantum computer also implies that it is not possible to predict results of a quantum system. There by implying that a quantum system is Probabilistic.

C. Entanglement

A quantum system may also exhibit the property of entanglement. It means qubits in a superposition are correlated with one and another. They cannot be described independent of each other. Quantum teleportation, an important concept in the field of quantum cryptography, depends upon entangled quantum states to deliver quantum information accurately and over relatively long distances.

II. QUANTUM WORLD V/S CLASSICAL WORLD

A quantum computer exhibits property of superposition and entanglement. Thus performing large number of reversible computations at the same time and then interfering all the results to get a single answer, makes a quantum computer powerful than a classical computer.

Also a Classical Computer picks up possible computations paths, "what-could-happen-but-did-not" has no impact whatsoever on the outcome of computation. While quantum computers diagnostically manipulates many computational paths that can be put all together in a single piece of hardware. A quantum computer is a computer where the number of operations required to arrive at a conclusion is exponentially small. So the improvement is not in the speed of the individual operation, but it is in the need to arrive at the conclusion.[1]

 ISSN: 2454-4248
69 – 71

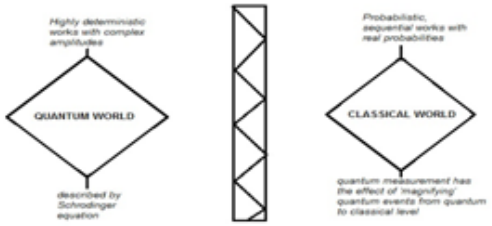

Figure 1 Taken from Ref [1]

III. QUANTUM ALGORITHMS

The quantum algorithm progresses on a logical composition of quantum physics. First of all, it activates the spread then encodes the problem and finally unleashes the power.

The commonly applied algorithms are Shor's algorithm for factorization, and Grover's algorithm for exploring an unregulated database or an unorganized list. [1] [2]

A. Shor's Algorithm

Shor's factorization algorithm is a quantum algorithm which is named after mathematician Peter Shor. This algorithm suggests that Quantum mechanics allow factorization in polynomial time instead of exponential time and this could have dramatic impact on the field of data security. This algorithm was developed for efficiently finding the prime factors of large numbers. Complexity of shor's algorithm is O(log N) while complexity of classical algorithm is O((log N)^k). Therefore this is considerably more efficient than known classical factorization algorithms

It is worth mentioning here that there are cryptographic systems, such as RSA, that are used extensively today and that are based on the conjecture that no efficient algorithms exist for solving the prime factorization problem. Hence, Shor's algorithm, if implemented on a large-scale quantum computer, would break the RSA cryptosystem. [1] [2]

B. Grover's Algorithm

Grover's algorithm searches for a specified item in an unstructured database, employing an important technique in quantum algorithm design known as amplitude amplification to achieve a polynomial speedup over the best classical algorithms. Grover's algorithm displays the correct answer with unique possibilities, exploring through an unregulated or unorganized databases or lists. [1] [4]

C. Boson's Sampling Algorithm

Boson sampling is a rudimentary quantum algorithm tai- lored to the platform of linear optics, which has sparked inter- est as a quick way to demonstrate such quantum supremacy [5]. Boson-sampling is a simple model for carrying out op- erations on Quantum Computers giving equitable sample for probability distribution randomly from large scattered data. Boson sampling algorithm will provide helpful information for developing quantum computers in near future than the algorithms laid so far.[3][2]

IV. BENEFITS

It has been shown that due to distinguishing properties, quantum computer operates much faster and therefore will per- form complex computation on huge amount of data in short interval of time. On the other hand, increasing the speed of computation also helps computer to learn faster even using the simplest methods. Due to quantum computer's high performance, Complex algorithms are being developed by researchers. Quantum bits also allow more information to be communicated per bit. Thus, it would enable the communication system in future to be dependable. [1] [2].

V. CONCLUSION

The quantum computer is based on theoretical concepts of quantum physics, making computer world more secure and less time consuming. Role of quantum computers is to provide assistance in capturing what is beyond the boundary imposed by time and energy needs. Perhaps, in the not so distant future, we will be able to climb up the ladder to a new rung of possibilities, such as the creation of the new drugs, breakthroughs in research of climate change, and the developments of new technological devices. Hence, this paper will benefit the researchers in further discussion in the field of Quantum Computers.

 ISSN: 2454-4248
69 – 71

ACKNOWLEDGMENT

The authors would like to thank their mentor Mr. Riju Bhattacharya for useful discussions and suggestions.

REFERENCES

[1] J. Gruska, Quantum Computing (McGraw-Hill publications). edition, 1999.

[2] S. A. Malinovskaya and I.Novikova, "From atomic to mesoscale: The role of quantum coherence in systems

[3] of various complexities." world Scientific publishing Co. Ltd, 2015.

[4] "https://arxiv.org/ftp/cs/papers/0405/0405004.pdf."

[5] "https://www.nature.com/articles/nphys4270." [Online].

[6] "https://people.cs.umass.edu/." [Online].

[7] S. Shannon, "Trends in quantum computing research." Nova SciencePublishers .Inc., 2006.

AUTHOR PROFILES

Anisha Sharma is a Computer Science & Engineering student currently pursuing her Engineering degree from Shri Shankaracharya Institute of Professional Management & Technology, Raipur. Her areas of interests and research include Quantum computers.

ANUBHA DATEY IS A COMPUTER SCIENCE & ENGINEERING STUDENT currently pursuing her Engineering degree from Shri Shankaracharya Institute of Professional Management & Technology, Raipur. Her areas of interests and research include Quantum computers.