IJRESM
International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Quantum Computing

Ramveer Singh Yadav[1], Sumit Kumar Saini[2], Vashu Malik[3]
[1]Assistant Professor, Department of CSE, Babu Banarasi Das Institute of Technology, Ghaziabad, India
[2,3]Student, Department of CSE, Babu Banarasi Das Institute of Technology, Ghaziabad, India

***Abstract*: Modern computer use 0 and 1 as input called bit to process data and an ALU (arithmetic logic unit) which has module to perform operation some basic operation such as addition, multiplication. With the help of modules a computer can perform small calculation of adding to numbers and large calculation of astrophysics. But in order to perform large calculations we need few thousand line of code and a army of experts people. As classical computer use addition operation as basic module it can't solve problems which blows up exponentially like problem of factorization, stimulation of molecule, Cryptographic algorithms. The answer to such problem is quantum computing and to create one we have to go subatomic which is physical boundary for us. Because only quantum world possess such properties which are required to create a quantum computer. Such a computer is different from binary digital electronic computer based on transistor. Quantum computing takes advantage of the strange ability of subatomic particles to exist in more than one state at any time. Where a 2-bit register in an ordinary computer can store only one of four binary configurations (00, 01, 10, or 11) at any given time, a 2-qubit register in a quantum computer can store all four numbers simultaneously.**

***Keywords*: Qubit, Quantum Mechanics, Entanglement, Super position, Interference.**

1. Introduction

As our ancestors do not possess any special physical quality except intelligence so they begins to develop tools. The human evolution led the emergence of modern human. We had invented things such as medicines, cars, airplanes, battle tanks, etc. But the discovery of classical computer created a bench mark in the history of human kind. The first electrical computer had a very large size consisting a size of room and perform some basic calculation and consume huge amount of power. In coming years its size is reduced to a laptop its performance is increased. Modern computer use transistors which help in reducing size as it eliminate the vacuum tube. Modern computer use 0 and 1 as input called bit to process data and a ALU (arithmetic logic unit) which has module to perform operation some basic operation such as addition, multiplication. With the help of modules a computer can perform small calculation of adding to numbers and large calculation of astrophysics. But in order to perform large calculations we need few thousand line of code and an army of expert's people. As classical computer use addition operation as basic module it can't solve problems which blows up exponentially. The answer to such problem is quantum computing and to create one we have to go subatomic which is physical boundary for us. Because only quantum world possess such properties which are required to create a quantum computer.

2. History

In 1982, physicist Richard Feynman proposed the idea of creating machines based on laws of quantum mechanics. In 1985, David Deutsh published a paper in which he describes about the universal quantum computer. In 1994, Peter Shor derived the first quantum algorithm, to factor the large numbers in polynomial time. He used entanglement and superposition properties of quantum mechanics to find the prime factors of integers which are used in the quantum encryption technology. To uncover this topic we have to understand following things:

Superposition

Quantum world is pretty weird place which is beyond understanding of human. Superposition is a state of electron in quantum world due to which it exhibit two states at the same time. Electrons, and all other fundamental particles, have a property known as "spin". Changing the electron's spin from one state to another is achieved by using a pulse of energy, such as from a laser - let's say that we use 1 unit of laser energy. But what if we only use half a unit of laser energy and completely isolate the particle from all external influences? According to quantum law, the particle then enters a superposition of states, in which it behaves as if it were in both states simultaneously.

A. Entanglement

Particles (such as photons, electrons, or qubits) that have interacted at some point retain a type of connection and can be entangled with each other in pairs, in a process known as correlation. Knowing the spin state of one entangled particle - up or down - allows one to know that the spin of its mate is in the opposite direction. Even more amazing is the knowledge that, due to the phenomenon of superposition, the measured particle has no single spin direction before being measured, but is simultaneously in both a spin-up and spin-down state.

B. Qubit

A qubit or quantum bit is the basic unit of quantum information—the quantum version of the classical binary bit physically realized with a two-state device. A qubit is a two-state (or two-level) quantum-mechanical system, one of the simplest quantum systems displaying the weirdness of quantum mechanics. Where a 2-bit register in an ordinary computer can store only one of four binary configurations (00, 01, 10, or 11) at any given time, a 2-qubit register in a quantum computer can store all four numbers simultaneously.

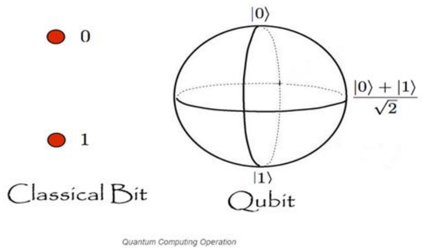
0
1
Classical Bit
$|0\rangle$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$
Qubit
Quantum Computing Operation

Fig. 1. Quibit

C. *Interference*

'Interference' refers to the electrons - which behave as waves inside a quantum waves, interference patterns which give rise to the quantum effects.

3. Quantum computing

Quantum computing is the area of study focused on developing computer technology based on the principles of quantum theory, which explains the nature and behavior of energy and matter on the quantum (atomic and subatomic) level. It basically involve the computing of the quantum mechanical phenomena, such as superposition and entanglement. A quantum computer is a device that performs quantum computing. Such a computer is different from binary digital electronic computer based on transistor. In classical computing, a bit is a single piece of information that can exist in two states – 1 or 0. Quantum computing uses quantum bits, or 'qubits' instead. Qubits are quantum systems with two states at the same time. However, unlike a usual bit, they can store much more information than just 1 or 0, because they can exist in any superposition of these values. Quantum computing takes advantage of the strange ability of subatomic particles to exist in more than one state at any time. Due to the way the tiniest of particles behave, operations can be done much more quickly and use less energy than classical computers.

A. *Quantum computer*

A quantum computer is any device for computation that makes direct use of distinctively quantum mechanical phenomena, such as superposition and entanglement, to perform operations on data. In a classical (or conventional) computer, information is stored as bits but in a quantum computer, it is stored as qubits (quantum bits).The basic principle of quantum computation is that the quantum properties can be used to represent and structure data, and that quantum mechanisms can be devised and built to perform operations with this data. Although quantum computing is still in its infancy, experiments have been carried out in which quantum computational operations were executed on a very small number of qubits. Research in both theoretical and practical areas continues at a frantic pace, and many national government and military funding agencies support quantum computing research to develop quantum computers for both civilian and national security purposes, such as cryptanalysis. If large-scale quantum computers can be built, they will be able to solve certain problems exponentially faster than any of our current classical computers (for example Shor's algorithm). The power of quantum computers Integer factorization is believed to be computationally infeasible with an ordinary computer for large integers that are the product of only a few prime numbers (e.g., products of two 300-digit primes). By comparison, a quantum computer could solve this problem more efficiently than a classical computer using Shor's algorithm to find its factors. This ability would allow a quantum computer to "break" many of the cryptographic systems in use today, in the sense that there would be a polynomial time (in the number of bits of the integer) algorithm for solving the problem. In particular, most of the popular public key ciphers are based on the difficulty of factoring integers, including forms of RSA. 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. The only way to increase the security of an algorithm like RSA would be to increase the key size and hope that an adversary does not have the resources to build and use a powerful enough quantum computer.

B. *Some obstacle in production of quantum computer*

- *Interference* - During the computation phase of a quantum calculation, the slightest disturbance in a quantum system (say a stray photon or wave of EM radiation) causes the quantum computation to collapse, a process known as de-coherence. A quantum computer must be totally isolated from all external interference during the computation phase. Some success has been achieved with the use of qubits in intense magnetic fields, with the use of ions.
- *Error correction* - Because truly isolating a quantum system has proven so difficult, error correction systems for quantum computations have been developed. Qubits are not digital bits of data, thus they cannot use conventional (and very effective) error correction, such as the triple redundant method. Given the nature of quantum computing, error correction is ultra critical - even a single error in a calculation can cause the validity of the entire computation to collapse. There has been considerable progress in this area, with an error correction algorithm developed that utilizes 9 qubits (1 computational and 8 correctional). More recently, there was a breakthrough by IBM that makes do with a total of 5 qubits (1 computational and 4 correctional).
- *Output observance* - Closely related to the above two, retrieving output data after a quantum calculation is

complete risks corrupting the data. In an example of a quantum computer with 500 qubits, we have a 1 in 2^500 chance of observing the right output if we quantify the output. Thus, what is needed is a method to ensure that, as soon as all calculations are made and the act of observation takes place, the observed value will correspond to the correct answer. How can this be done? It has been achieved by Grover with his database search algorithm that relies on the special "wave" shape of the probability curve inherent in quantum computers that ensures, once all calculations are done, the act of measurement will see the quantum state decohere into the correct answer.

4. Quantum computer hard ware

A. Quantum transistor (SQUID)

SQUID stands for Superconducting Quantum Interference Device which uses interference that is one kind of quantum effect which make it possible to use atom as 'qubit'. Using the quantum mechanics that is accessible with these structures, we can control this object so that we can put the qubit into a superposition of these two states as described earlier.

B. Computer cooling

Reduction of the temperature of the computing environment below approximately 80mK is required for the processor to function, and generally performance increases as temperature is lowered - the lower the temperature, the better. To reach the near-absolute zero temperatures at which the system operates, the refrigerators use liquid helium as a coolant. The specialized equipment to allow cooling to these temperatures is available commercially and runs reliably. The computer can be cooled down to operating temperature within several hours, and once this temperature is reached remain cold for months or years.

C. Shielding

In addition to the magnetic shielding, the system sits inside a shielded enclosure which screens out RF electromagnetic noise. The only path for signals between the inside and outside of the shielded enclosure is a digital optical channel carrying programming information

5. Applications of quantum computing

- *Factorization:* For classical computer, the integer factorization of large integers (product of prime numbers) is difficult. But quantum computers can solve this problems using shor's algorithm. So the quantum computers can used in cryptographic applications. It is useful for encoding and decoding of secret information. It is highly secure. The third party cannot read the message. The current encryption methods are simpler. So the information sent through internet are not safe. Quantum computer can easily break the encrypted messages used today.
- *Discovery of new drugs.* Molecular simulations helps pharmacists and chemists to study about the interaction of products with each other and with biological processes.eg:- drug interact with disease. Chemists have to test the several molecular combinations for finding the best one which can prevent disease. It is an expensive process and also needs many years. By using the quantum computing, it try different molecular combinations and find the best one. It will reduce the cost and time for developing new drugs.
- *Space exploration*- Using Keplers space telescope, astronomers discovered over 2000 planets outside our solar system. The quantum computer can spot more planets and give more information using the telescopic images.
- *Artificial Intelligence* -Quantum computer can learn from experience. It can self-correct and even modify the program code. The machine learning ability of quantum computer help to do things faster and efficiently. It can used for artificial intelligence experiments. NQAIL (New Quantum Artificial Intelligence Lab) at NASA's Ames research centre in silicon valley will be operated by NASA, Google and USRA. Google and NASA use the quantum computer for developing more advancements in Artificial Intelligence.

6. Conclusion

This paper presents an overview of quantum computing

References

[1] https://en.wikipedia.org/wiki/Quantum_computing
[2] https://www.mepits.com/tutorial/355/trending-technologies/quantum-computing
[3] https://whatis.techtarget.com/definition/quantum-computing
[4] Michele Mosca, Phillip Kaye, and Raymond Laflamme "An Introduction to Quantum Computing 1st Edition.