M.Prasanth, S.Sathiyapriya, M.Preetha, Peri Institute Of technology, computer science engineering, Mannivakkam, Chennai-600048

***ABSTRACT-***

**In the developing field of technology the role of computers are vital but as the technology improves real life challenges also gets increased so normal computers find it difficult solve all those problem ,still there are many problem that exist which could take years to solve by an ordinary computer even super computers . To solve this problem there exist QUANTUM COMPUTERS.**

**The main goal of this presentation is to explain what is Quantum computer? By explaining its construction and principles behind these quantum computer along with the properties of Superposition, tunneling, entanglement, multiverse and the key component of quantum computer called quantum bits. The actual power of quantum computers and countless possibilities of it. We are going to see how the real time complex problem could be solved by the quantum computer. We are also going to see Google’s Quantum** **computers and what is QUANTUM SUPERMACY? How Google achieved its QUANTUM SUPERMACY. The future of technological world with Quantum computer and the areas where we are going to use these quantum computer in future**

**Quantum computers are the next generation of the technological world which has a great scope in finding solution for unsolvable problem and creating cryptography solutions**

*Keywords-*

Quantum mechanics, Quantum computers, Quantum computing, Quantum Bits, Superposition, Entanglement, Multiverse, Tunneling, Quantum Circuits, Quantum Supermacy, Sycamore Processor

1. INTRODUCTION

In the introduction part of this paper we will see the major aspects of the conventional computers. The conventional computers have few components that makes it slow compared to the quantum computers. The quantum computers are capable of completing things faster than the conventional computers with the greater difference.

The quantum computers uses quantum mechanisms for its computation moreover the quantum computers are difficult to assemble and the atmosphere where the quantum computers works need to be in extremely low temperature. The average temperature maintained is 0.015K. This low temperature could be maintained only by the liquefied helium. The Key difference between the conventional computer and the quantum computer is that quantum computer uses Quantum bits which is capable of being in two states at the same time, Where as in conventional computers the ordinary bits are used which has the capability of being in only one state at the time (0/1) .

1. QUANTUM COMPUTING

A.History

The first concept of using quantum mechanics in technology field was formulated in the year 1980 by the American physicist Paul. A Benioff. He proposed the quantum mechanical model of the Turing machine which uses the quantum bits rather than using the ordinary bits which provided infinite tape symbols.

Later [5] the idea of quantum computer was suggested by Mathematician Yuri Mannin in the year 1980, after that another American physicist Richard Philips Feynman provided the logical idea for quantum computer by his path integration formula of quantum mechanics in the year 1981.

They both found that quantum computers could be used to solve the problem that are out of reach for the normal computers. The power of quantum computer became known to everyone in the year 1994 when peter shor developed a polynomial quantum time algorithm which mainly focuses on factoring integers. This made a breakthrough by creating a vulnerability to an asymmetric key exchange RSA which is based on factoring integers. For breaking a RSA cryptography method it will took many years for the existing super computers and conventional computers

B. Parts of the quantum computer

The typical quantum computer constitutes of 4 parts and these 4 parts have an individual functionalities

1 .QUANTUM DATA PLANE-

The quantum data plane is the “heart” of a QC. It includes the physical quantum bits and the structures needed to hold them in place. It also must contain any support circuitry needed to measure the quantum bits’ state and perform gate operations on the physical quantum bits for a gate-based system or control the Hamiltonian for an analog computer.

2 .CONTROL AND MEASUREMENT PLANE-

The control and measurement plane converts the control processor’s digital signals, which indicates what quantum operations are to be performed, to the analog control signals needed to perform the operations on the quantum bits in the quantum data plane. It also converts the analog output of measurements of quantum bits in the data plane to classical binary data that the control processor can handle

3. CONTROL PROCESSOR PLANE AND HOST PROCESSOR-

The control processor plane identifies and triggers the proper Hamiltonian or sequence of quantum gate operations and measurements (which are subsequently carried out by the control and measurement plane on the quantum data plane). These sequences execute the program, provided by the host processor, for implementing a quantum algorithm. Programs must be customized for the specific capabilities of the quantum layer by the software tool stack.

One of the most important and challenging tasks of the control processor plane will be to run the quantum error correction algorithm

4. QUANTUM BIT TECHNOLOGIES-

Quantum bits are the key aspect of the quantum computers. The more research on the Quantum bits is implemented after shore’s algorithm on polynomial time

The quantum Technology mainly handles with two properties superconducting and trapped ion quantum bits

1. QUANTUM BITS AND QUANTUM CIRCUITS

A.QUANTUM BITS-

The quantum bits are the basic unit of the quantum information. The quantum information is the information about the state of the quantum system. The quantum bit is a two state quantum mechanical system. The great example for the quantum states is the polarization of photon in which two states can be taken either the vertical polarization or the horizontal polarization. Quantum mechanics allows the quantum bit to be in a coherent superposition of both states/levels simultaneously, a property which is fundamental to quantum mechanics and quantum computing. a quantum bit can hold more information, e.g. up to two bits using super dense .

For a system of *n* components, a complete description of its state in classical physics requires only *n* bits, whereas in quantum physics it requires 2*n*−1 complex numbers

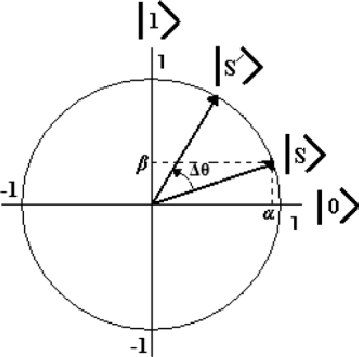


Figure1. Quantum bit

B. QUANTUM CIRCUITS

Large number of quantum gates are grouped together to form a quantum circuit as we do in the normal computers. The main difference between a quantum computer and a normal computer in circuits is in normal computers the logical gates are used to form the circuits but in the quantum computers the quantum gates are used

QUANTUM GATES-

The [2] quantum gates are capable of handling quantum bits and depending upon the quantum bits in the system the quantum gates are used and complexity of the system is also determined. Unlike other logical gates quantum gates are reversible that is the certain-extent of time is reversible.

The quantum logic gates are represented as unitary matrix. The number of quantum bits in the input and output of the gate must be equal a gate which acts on *n* {\displaystyle n}quantum bits is represented by a {\displaystyle 2^{n}\times 2^{n}} unitary matrix. The quantum states that the gates act upon are vectors in {\displaystyle 2^{n}} complex dimensions. Quantum states are typically represented as brackets.

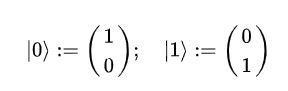


Fig2. Representation of a single quantum bit

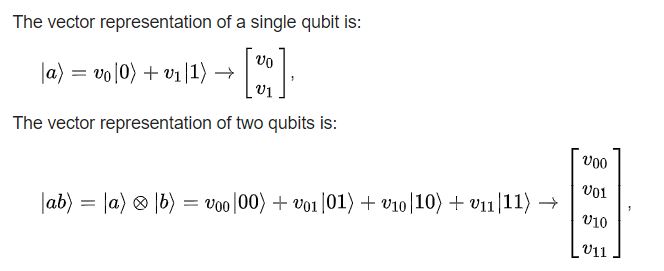
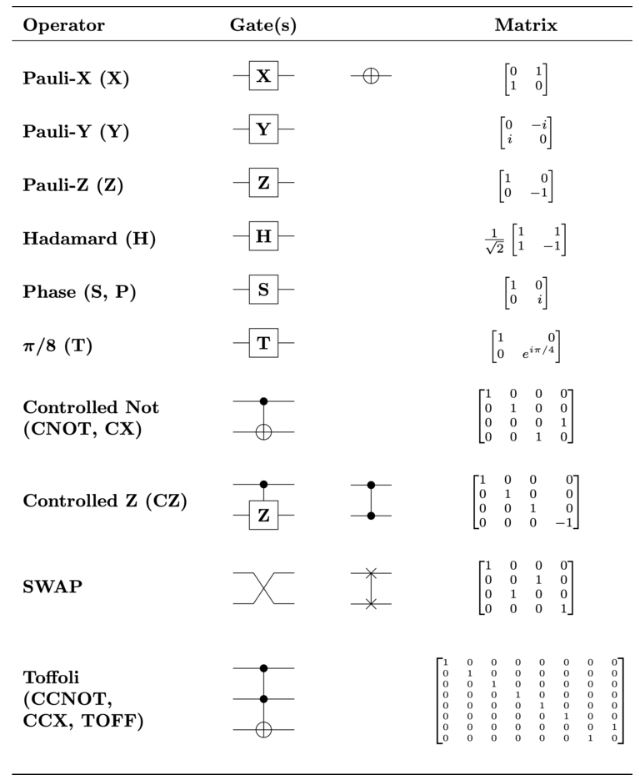


Fig.3. Representation of two quantum bit

The fig4 consists of quantum gates that are used in an quantum circuits these quantum gates has a matrix view with which we can obtain a meaning full result.

Universal quantum gates is any set of gates to which any operation possible on a quantum computer can be reduced, that is, any other unitary operation can be expressed as a finite sequence of gates from the set. Technically, this is impossible with anything less than an uncountable set of gates since the number of possible quantum gates is uncountable, whereas the number of finite sequences from a finite set is countable. To solve this problem, we only require that any quantum operation can be approximated by a sequence of gates from this finite set.

Fig.4. Quantum gates

So far we have not shown how quantum circuits are used to perform computations. Since many important numerical problems reduce to computing a unitary transformation *U* on a finite-dimensional space. One might expect that some quantum circuit could be designed to carry out the transformation *U*. In principle, one needs only to prepare an *n* quantum bit state ψ as an appropriate superposition of computational basis states for the input and measure the output *U*ψ. Unfortunately, there are two problems with this.

One cannot measure the phase of ψ at any computational basis state so there is no way of reading out the complete answer. This is in the nature of the quantum measurement. There is no way to efficiently prepare the input state ψ.

This does not prevent quantum circuits for the discrete Fourier transform from being used as intermediate steps in other quantum circuits, but the use is more subtle. In fact quantum computations are *probabilistic*.

1. QUANTUM COMPUTATIONAL PRINCIPLES

There [1]are four main quantum principles that are followed in the quantum computation these principles are necessary in the polarization of the quantum bits to either one or zero to get the desired output

1. SUPER POSITION-

Superposition is essentially the ability of a quantum system to be in multiple states at the same time that is one and zero at the same time.

1. ENTANGLEMENT-

Quantumentanglement is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated. This leads to correlations between observable physical properties of the systems.

1. MULTIVERSE-

Multiverse is the property that is evolving in the quantum computer which states the communication between the quantum computers to communicate with other computers.

1. TUNNELING-

Tunneling is the process of passing the quantum particle in the narrow tube to get polarized which results in the zero or one. Usually the quantum particles are made to pass through the potential barrier which is nothing but the wave mechanical reflection

1. QUANTUM SUPERMACY

The [3] aspect of this paper is quantum Supermacy. Before we get know what is a quantum computer. The concept of Quantum Supermacy is that making the quantum computer to work till it reaches its maximum capability.

Simply to say the quantum computer could solve the problem in 200seconds what an average computer would take 10000years to solve the same problem.

Google was the first organization to achieve the quantum Supermacy. The processor used by Google to achieve this is called as Sycamore processor. The key company behind this achievement was a Canadian quantum company called D-wave. This company at the beginning produced a quantum computer with only 16quantum bits but the quantum computer Google has is composed of nearly 54 quantum bits and this company also manufacture computers to organizations such as NASA, UNIVERSITY OF SOUTHERN CALIFORNIA.

So when we came to this particular question what quantum Supermacy means?

“Quantum Supremacy is the goal of demonstrating that a programmable quantum device can solve a problem that classical computers practically cannot.”

The difficult task here is finding the problem that could not solved by the conventional computers rather than building the quantum computer.

The problem taken by Google to prove the quantum Supermacy is to prove the random numbers generated by the quantum computers is random, to prove this the conventional computers will take lots of time because the sequence of random grow in turn. This problem is the kind of the exponential problem

There are certain proposals available to achieve the quantum Supermacy

1. A clearly defined computational problem
2. The quantum algorithm to solve the problem
3. A comparison algorithm to view the best case and worst case scenarios
4. A complexity theoretic argument
5. POWER OF QUANTUM COMPUTERS

This superposition of quantum bits is what gives quantum computers their inherent parallelism. According to physicist David Deutsch, this parallelism allows a quantum computer to work on a million computations at once, while you’re desktop PC works on one. A 30-qubit quantum computer would equal the processing power of a conventional computer that could run at 10 teraflops (trillions of floating-point operations per second). Today's typical desktop computers run at speeds measured in gigaflops (billions of floating-point operations per second).

The quantum computer could provide the strongest cryptographic techniques which will take years to solve by hackers using there devices, if they want to hack them then the only option is to they need to try with a quantum computer which is not a possible option.

The computer has the capability to create great achievements in cryptography, weather forecasting, drugs, and space related researches.

Let’s have an example to understand the power of the quantum computer

Imagine there are three people x, y, z, and we need to book two taxi’s the task here for us is we need to split the people into two groups but there is a condition

* X and Y are friends
* X and Z are enemies
* Y and Z are friends

We need to focus on two things

* Maximize the number of **friend pairs**that share the same car
* Minimize the number of **enemy pairs**that share the same car

Now for this problem when we use conventional computers we have 8 pairs of possibilities and these possibilities can be expressed in 3 bit pairs. So by checking the possibilities one by one we could solve the problem imagine there are 1000people and for a conventional computer it is difficult to solve this scenario

When we use quantum computers

For the 3 bits of possibilities it is enough to have only 3 quantum bits and to have all the 8 possibilities at the same time

1. FUTURE

pharmaceutical companies could accelerate the discovery of new drugs, materials companies could discover new molecular structures, finance companies could develop new trading strategies, transportation companies could optimize logistics, and companies relying on the output of machine and deep learning could perform analyses that are impossible with classical computing of today

* Airlines seeking the optimal way to store spare parts at airports.
* Distribution centers wanting the best way to maneuver robotics around a warehouse.
* Oil and gas companies calculating how atoms and molecules can be configured to protect equipment from corrosion.
* [4] Improving encryption technology by generating random numbers. Google's quantum team is talking to its encryption key generation team about using a random-number generation tool it's already developed for today's Sycamore machine.
* Building machine learning systems better at tasks like distinguishing between real and fake items like bogus political videos. This was the original impetus for Neven's work, and Google researchers think it could be the first area to deliver on quantum computing's promise.
* Complicated optimization problems, such as calculating how to deliver packages in the shortest time while using the least energy. "Optimization problems occur everywhere at every company anywhere in the world," Bacon said. Addressing those challenges could both save money and help the environment.

REFERENCES

[1]<https://www.nap.edu/read/25196/chapter/7#114>

[2]<https://en.wikipedia.org/wiki/Quantum_logic_gate>

[3]<https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing>

[4]<https://www.cnet.com/news/google-quantum-supremacy-only-first-taste-of-computing-revolution>

[5]<https://en.wikipedia.org/wiki/Quantum_computing>