JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Gist on Quantum Computing

Sripriya Simhadri

Application Engineer 2, Oracle India Private. Ltd, Hyderabad, Telangana, India. sripriya.simahadri@gmail.com.

Abstract:

Over the last three decades computers have become exceptionally compact and faster. Now that we have reached the fifth generation of computers which include concepts of artificial intelligence, what's next? There is a lot of fuss about quantum computers being a strong contender for the next generation of computing. Recently we heard stories about small scale quantum computers being built by technology giants like IBM and Google and also an instance of quantum supremacy.

One of the key features of quantum computing is its core concept, leveraging the principles of quantum mechanics, which we have avoided with our classic computers. Quantum computers are the first ones to deviate from the basic concept of bits. To understand this difference in the fundamental concepts, we start with basic building blocks in conventional computers, bits and draw contrasts with those in quantum computers. Further explore how rudimentary operations are performed in both machines by comparing addition operations of 2 and 3 bits. Followed by a brief detail on current research on quantum computers and claims on their supremacy over current machines. Then we elaborate on the world of new possibilities and unsolvable problems quantum computers have the ability to tackle.

This paper aims at giving a gist of quantum computing to beginners, starting with fundamentals to current research by identifying stark contrasts with conventional machines. It also explores the need of new computation powers and why we have reached almost the tail end of processing power of classical computers.

KEY WORDS: Conventional computers, transistors, logic gates, half adder, full adder, quantum mechanics, quantum computing, Qubits, quantum supremacy.

1 INTRODUCTION

1.1 What is a computer?

The computer is a complex machine that can solve many problems more rapidly, precisely, or accurately than a human. It takes input from the user and processes this data under the control of a set of instructions , called a program to obtain the result and also has the capability to save it for future use.

1.2 Brief history of computer development.

Charles Babbage, considered by many as the father of computers, designed two computers, a mechanical computer called 'the difference engine' and 'analytical engine'. The difference engine was designed to calculate a series of values automatically, the main intent being able to solve polynomial functions. Though in the 1800s, this design was too large and expensive to be constructed, two models were later developed in late 1990s.

The analytical engine is the basis for Charles' standing as a computer pioneer. It was designed to use loops of punch cards, to control the mechanical computer, in addition to being capable of using result from previous computation in the next one,

Though not constructed in charles' lifetime, it formed the basis of modern computation principles.

Alan Turing is widely known as the father of theoretical computer science. His Turing Machine, considered a model of general-purpose stored programming computing fundementalized the concepts of algorithms and computation.

In ensuing decades computers leveraged millennia of mathematical and physical sciences research, coalescing it with latest discoveries to develop modern sophisticated machines. First generation vacuum tubes were replaced by smaller switches, called transistors. Integrated circuits encompassing multiple transistors and many other electronic components soon revolutionized computers. Followed by development of the microprocessors which give integrated circuit computational capabilities.

2 CONVENTIONAL COMPUTERS

2.1 How do classical computers work?

Let's start with how conventional computers work, they leverage the millennia of mathematical and physical sciences research. All conventional computers do two things

1. Store information in memory in the form of bits 1 and 0.
2. Then they process the said bits using various operations.

The basis of conventional computers lies in the ability of transistors having two states on and off.

2.2 Now that we have established what they do, let's look into how:

The basic building block of a computer is a transistor. A single modern CPU can have hundreds of millions or at times billions of transistors. Transistor is a switch made of silicon or some other semiconductor material that can change its electrical state when pulsed. In its normal state, the material may be non conductive or conductive, either impeding or letting current flow. When voltage is applied to the gate, the transistor changes its state.Like any other electronic device, in computers various transistors are connected together to form circuits, here referred to as logic gates.

2.3 A peep into basic logic gates and elaboration on addition operation.

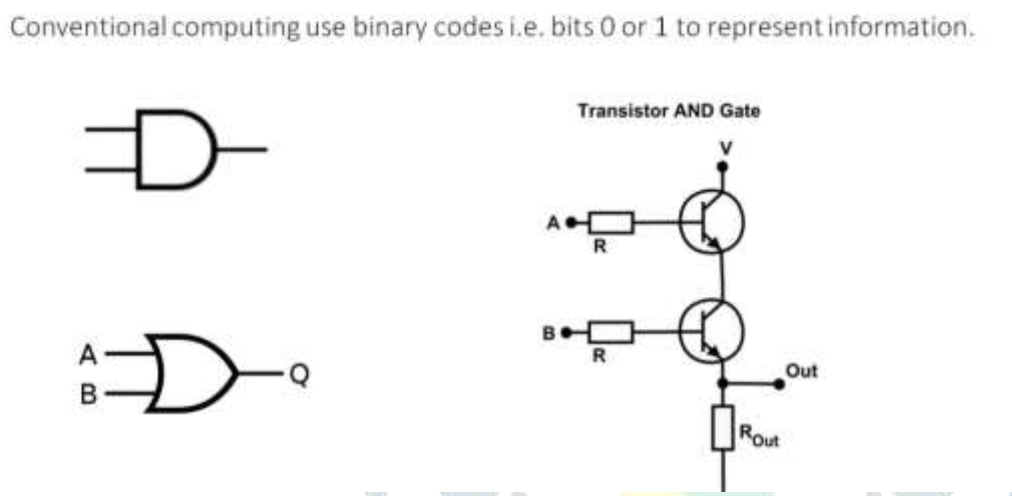

Fig.1 AND and OR logic gates, AND gate internal structure.

Figure 1 represents two basic computational logic gates- AND gate and OR gate. Both the gates take two bits as input and give a bit as output. Let's elaborate on AND gate functionality-

The basic principle of a transistor is that voltage or signal at its base allows flow of current from one terminal to another. In the case of AND gate, two transistor bases are connected to the input signals and each other.

Consider input A is 1,so some voltage is sent to transistor 1, which passes to one terminal of transistor 2. Now, if input B is also 1, current flows through transistor 2, resulting in an output of 1. On the contrary if input B is 0, current doesn't flow through the second transistor giving the result as 0.

Similarly, if input A is 0, no voltage is sent to transistor 1, hence none to transistor 2. Now, whatever input B is, since there is no voltage difference between two terminals of the second transistor, the result of the operation is zero.

The essence of computers revolves around different combinations of transistors used to build basic logic gates. These gates are arranged in countless permutations and combinations to perform many mathematical and storage operations.

Now, figure 2 also shows how AND and OR gates are arranged to perform addition operation.

A half adder is an electronic circuit that performs the addition of numbers. It adds two single binary digits and provides the output plus a carry value. A half adder can be built with two or three logic gates, AND gate being mandatory, it can use an Exclusive OR[XOR] or a combination of OR gate and NOT gate. If A and B are 1, the sum will be NOT(A OR B) or A XOR B resulting in 0 and carry will be A AND B which is 1.

A full adder circuit is central to most digital circuits that performs addition or subtraction. It extends the concept of the half-adder by providing an additional carry-in (Cin) input. It is so called because it adds together two binary digits, plus a carry-in digit to produce a sum and carry-out digit. It therefore has three inputs and two outputs.

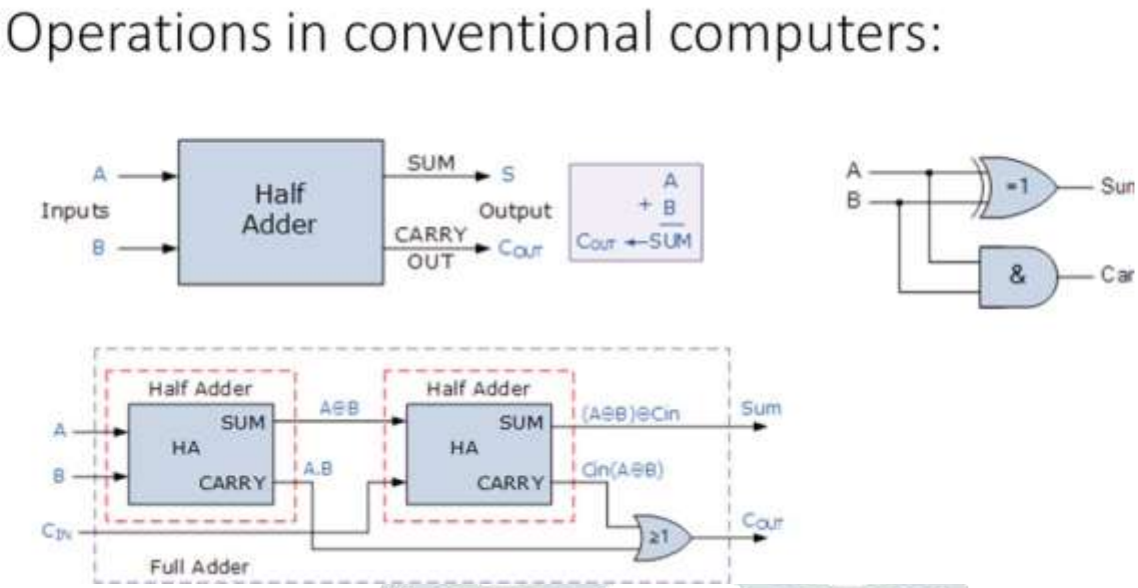

Fig.2 Half Adder and Full Adder

2.4 Moore's Law:

Early computers were huge and expensive. ENIC, the first digital computer, weighed around 30 short tons occupying 1800 square meters. Construction of low cost and compact hardware is to be credited for development of computational devices like smartphones that are small enough to fit in pockets over the past few decades.

Gordon Moore, co-founder of Intel, predicted integrated circuits are a path to cheaper electronics- the number of transistors in a dense integrated circuit (IC) would double every year for the next decade, based on the economics of the integrated circuit. Moore wrote: "The cost per component is nearly inversely proportional to the number of components," so the more the number of transistors, the lower the cost per transistor.

Moore's predictions were based on the innovations in development of integrated circuits, which emerged as an unplanned advance amid efforts in the late 1900s to improve transistor manufacturing. Transistors were used as switches and amplifiers in radios, televisions and early computers. The first of these innovations is the planar process, which created operable transistors by fabricating them on the surface of flat silicon pieces. This process led to fabrication of multiple transistors on a single piece of silicon. Then came the invention of a means to connect transistors on the silicon surface to form a circuit. Since the transistor circuit was integrated on a silicon surface, the name 'integrated circuit' came. The architecture of integrated circuits became complex with time, now is a type of layered printing process, where transistors are printed successively on a series of layers. The process of IC manufacture takes the same amount of time regardless of the number of transistors in the circuit, as a result production cost is determined by the size of silicon wafer.

Moore, then an employee at Fairchild semiconductors, examined the cost of integrated circuits and noticed that, owing to design and processing improvements, the number of transistors that can be printed on each IC is increasing exponentially over time as in doubling every year. It turned out to be an accurate prediction for the next ten years eventually this insight became a prediction, which inturn became the golden rule known as 'Moore's Law'. He later revised his prediction, stating the number of transistors would double every two years moving forward.

Moore's Law applied widely till early 2010s, making more or less accurate predictions about the number of transistors that could fit on an integrated circuit. However, over the last few years, growth of the number of transistors on each IC is declining and falling much lower than what Moore's law predicts. Many computer scientists and Moore himself predicted that the law was coming to an end.

2.5 Factors leading to end of Moore's law:

Despite the remarkable efforts of research engineers, you can only make transistors so small before you run out of room at the bottom. Go much smaller than this and the transistors become so tiny that the effects of quantum physics start to interfere electrons start to jump around and turn up in places where you don't want them to be. With so little space, it also becomes difficult to organise the fine structure of the silicon wafer that's essential to control its electrical properties. Pack in too many transistors and make them work faster and the restricted flow of electrons within the chip can make it so hot that without significant cooling, it will burn itself up.

2.5.1 Electrical leakage: Over the years, transistors have not only gotten smaller but also became extremely efficient. However, they reached the physical limitation called 'Dennard Scaling' which states, as transistors get smaller their power density stays constant. Transistors have gotten as small as 7-10 nanometers that the channel that carries the electrical current through the transistor may not be able to contain it. This generates heat which can wear out the transistors more quickly, making them even more susceptible to leakage. Heat isn't just limited to one transistor though.Billions of transistors leaking can seriously threaten the integrity of the whole chip, so the processor must reduce the amount of voltage it takes in or throttle the number of transistors in use to prevent overheating, limiting the processing power of the chip. Because of the breakdown of Dennard scaling, miniaturization is now full of trade-offs. Making a transistor smaller no longer makes it both faster and more efficient. In fact, it's very difficult to shrink today's transistors and maintain even the same speed and power consumption of the previous generation.

2.5.2 Effective oxide layer: In transistors, for the gate voltage to effectively modulate the channel electric potential, i.e. to turn off the transistor when the gate voltage is low, the gate-to-channel capacitance must be maximized. This has historically been achieved by reducing the thickness of the effective oxide layer; it is less than 2 nm in today's state-of-the-art technology. Unfortunately, further gate oxide thickness scaling is limited due to the dramatic increase in gate leakage current brought about by quantum-mechanical tunneling.

2.5.3 Economy: When the number of transistors doubles, so does the amount of heat they can generate. The cost of cooling large server rooms is getting more and more untenable for many businesses who are the biggest purchasers of the most advanced processing chips. Transistors are actually printed onto silicon chips, not with a printing press but with lithography, using exotic chemicals and materials in a chip fabrication plant called the "fab". Packing more transistors in each generation of chips requires the fab to shrink the size of the transistors. The first transistors were printed with lines 80 microns wide. Today Samsung and TSMC are pushing to produce chips which are a few dozen nanometers across.That's about a 2,000-to-1 reduction. Each new generation of chips that shrinks the line widths requires fabs to invest enormous amounts of money in new chip-making equipment. While the first fabs cost a few million dollars, current fabs are over $10 billion.

3 QUANTUM COMPUTERS

3.1 Quantum Mechanics:

Quantum mechanics explains the behavior of matter and its interactions with energy on the scale of atomic and subatomic particles. In classical mechanics, objects exist in a specific place at a specific time. However, in quantum mechanics, objects instead exist in a haze of probability; they have a certain chance of being at point A, another chance of being at point B and so on. Light in some aspects has behaviour like particles and in others it behaves like waves. Matter in the universe consisting of particles such as electrons and atoms sometimes exhibits wavelike behavior as well.. Quantum mechanics shows that light, along with all other forms of electromagnetic radiation, comes in discrete units, called photons, and predicts its spectral energies and the intensities of its light beams. A single photon is a quantum, or smallest observable particle, of the electromagnetic field. More broadly, quantum mechanics shows that many properties of objects, such as position, speed, and angular momentum, that appeared continuous in the zoomed-out view of classical mechanics, turn out to be quantized. Such properties of elementary particles are required to take on one of a set of small, discrete allowable values, and since the gap between these values is also small, the discontinuities are only apparent at very tiny scales. Many aspects of quantum mechanics are counterintuitive and can seem paradoxical because they describe behavior quite different from that seen at larger scales. In the words of quantum physicist Richard Feynman, quantum mechanics deals with "nature as She is absurd".

Quantum interactions are quite unlike those experienced by people every day. Some of the defining principles of quantum mechanics are described below.

3.1.1 Wave-particle duality: A quantum object generally has both wave- and particle-like properties. While the evolution of the system follows a wave equation, any measurement of the system will return a value consistent with it being a particle.

3.1.2 Superposition: A quantum system can exist in two or more states at once, referred to as a "superposition" of states or a "superposition state." The wave function for such a superposition state can be described as a linear combination of the contributing states, with complex coefficients. These coefficients describe the magnitude and relative phases between the contributing states.

3.1.3 Coherence: When a quantum system's state can be described by a set of complex numbers, one for each basis state of the system, the system state is said to be "coherent." Coherence is necessary for quantum phenomena such as quantum interference, superposition, and entanglement. Small interactions with the environment cause quantum systems to slowly decohere. The environmental interactions make even the complex coefficients for each state probabilistic.

3.1.4 Entanglement: Entanglement is a special property of some (but not all) multiparticle superposition states, where measurement of the state of one particle collapses the state of the other particles, even if the particles are far apart with no apparent way to interact. This arises when the wave functions for different particles are not separable (in mathematical terms, when the wave function for the entire system cannot be written as a product of the wave functions for each particle). There is no classical analogue to this phenomenon.

3.1.5 Measurement: Measurement of a quantum system fundamentally changes it. In the case where the measurement yields a well-defined value, the system is left in a state corresponding to the measured value. This is commonly referred to as "collapsing the wave function."

Harnessing these properties in a controlled way creates new potential paradigms for engineering.

3.2 Quantum Computing:

The most familiar of all contenders looking to supersede conventional silicon chips is quantum computing. Instead of letting quantum effects prevent our tiny transistors from working, why not build devices that take advantage of the tiny quantum effects to make them work? Quantum computing leverages the concepts of quantum mechanics, i.e. the ability of particles to exist in more than one state at any given point of time.

Any computational problem that can be solved by a conventional computer can also be solved by a quantum computer. Conversely, any problem that can be solved by a quantum computer can also be solved by a classical computer, at least in principle given enough time. In other words, quantum computers obey the Church–Turing thesis. This means that while quantum computers provide no additional advantages over classical computers in terms of computability, quantum algorithms for certain problems have significantly lower time complexities than corresponding known classical algorithms.Quantum computers will not entirely replace our classical computers, their ability to solve complex problems will open up a new world of possible innovations.

3.3 Some problems quantum computing approach can solve effectively:

3.3.1 Optimizing exponential growth problems like supply chain:

Consider the problem of finding the route to the end of this puzzle, conventional computers pick and eliminate one path after another as shown in the image on the left, whereas quantum computers possess the capability to check different paths at same time, therefore solving the problem quicker as shown in Figure 4. Another problem that quantum computers could solve efficiently is A logistics company, delivering to 50 cities, wants to know the optimal route to save on fuel costs.

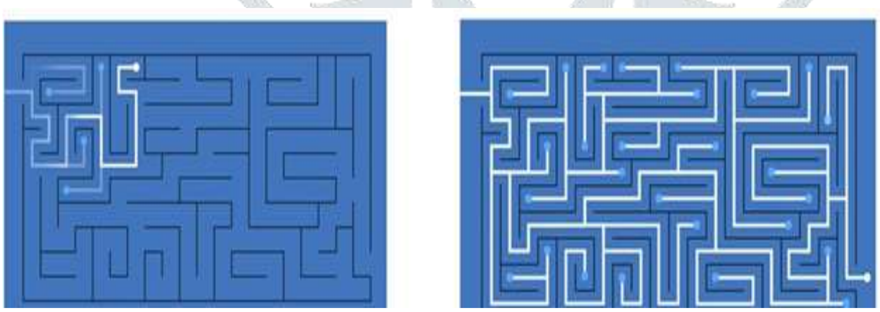

Fig.3 Puzzle solved by conventional and quantum computers

3.3.2 Chemistry and medicine:

Running searches on quantum computers could unfold looking through all possible chemical molecules with unimaginable speed, drug target tests conducted in every potential cell model or in silico human tissues and networks in the shortest amount of time possible. This would open the gates to find the antidote to diseases we never dreamt about before like Alzheimer's, various types of cancer.

It took more than 15 years to crack the code of the human DNA. Although the technical conditions, the time and the cost of sequencing genomes were reduced by a factor of 1 million in less than 10 years, the revolution lags behind. Quantum computing could give a significant push to the area: faster sequencing, as well as a more comprehensive and faster analysis of the entire genome, will be possible with it. Plus, predictions will be more reliable as quantum computers could take into account even more information as traditional computers, and they could even build every piece of genomic data into health records. Quantum computing could take out the guesswork from genomics and genetics for ensuring better health for everyone.

Quantum computing would take that to a whole new level and even augment it with special skills. What if such computers could offer perfect decision support for doctors? They could skim through all the studies at once, they could find correlations and causations that the human eye would never find, and it might stumble upon diagnosis or treatment options that the human doctor could have never figured out by themselves.

3.3.3 Weather Forecasting:

Currently, the process of analysing weather conditions by traditional computers can sometimes take longer than the weather itself does to change. But a quantum computer's ability to crunch vast amounts of data, in a short period, could indeed lead to enhancing weather system modelling allowing scientists to predict the changing weather patterns in no time and with excellent accuracy something which can be essential for the current time when the world is going under a climate change.

3.3.4 Cybersecurity & Cryptography

Cybersecurity has continued to be an essential concern around the world, but the process of developing encryption and security frameworks is becoming daunting and impractical for classical digital computers. With increased dependency on digitisation, the vulnerability to threats like cyber attacks. Quantum computing with the help of machine learning can help in developing various techniques to combat these threats. Additionally, quantum computing can help in creating encryption methods, also known as quantum cryptography.

3.4 How does quantum computing work?

3.4.1 Qubits:

A quantum bit, or qubit, has two quantum states, analogous to the classical binary states. While the qubit can be in either state, it can also exist in a "superposition" of the two. These states are often represented in Dirac notation, where the state's label is written between a | and a ⟩. Thus, a qubit's two component states are generally written as | 0 ⟩ and | 1 ⟩. Any given qubit wave function may be written as a linear combination of the two states, each with its own complex coefficient.

$$a_i: |\psi\rangle = a_0 |0\rangle + a_1 |1\rangle.$$

3.4.2 Bloch sphere:

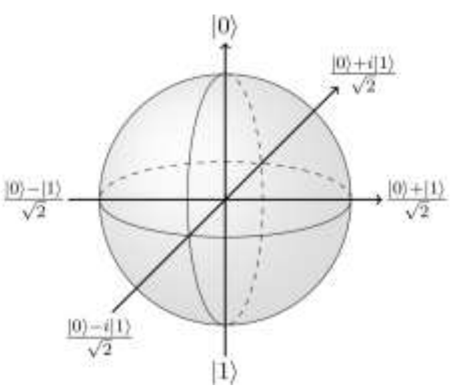

Fig.4 Bloch Sphere

In quantum mechanics and computing, the Bloch sphere is a geometrical representation of the pure state space of a two-level quantum mechanical system (qubit), named after the physicist Felix Bloch. A two-level system implies having two basic states, here a single qubit is in superposition of |0> and |1>. These two basic states are usually put at the north and south poles of the sphere and any other point corresponds to a certain superposition.

Figure 5 shows a bloch sphere, with states of superposition between |0> and |1>.

3.4.3 Superposition:

Now, this superposition is a gamechanger- four classical bits can be one of two power four configurations that is 16 combinations out of which it can be one at any point of time, however, four qubits in superposition can be in all of those combinations at once. This number grows exponentially with every additional qubit, twenty qubits can store two million values at once.

3.4.4 Quantum Entanglement:

An important distinguishing feature between qubits and classical bits is that multiple qubits can exhibit quantum entanglement. Quantum entanglement is a nonlocal property of two or more qubits that allows a set of qubits to express higher correlation than is possible in classical systems. It is a close connection that makes each of the qubits react to change in others state instantaneously no matter how far apart they are. This also implies while measuring just one entangled qubit, properties of it's partners can also be deduced.

3.4.5 Qubit manipulation using quantum gates:

In a gate-based approach to quantum computing, each primitive operation is performed by precisely changing the Hamiltonian of one or more qubits for the specific amount of time required to achieve the desired transformation. This is done by changing the physical environment, for example, via a laser pulse or application of some other electromagnetic field, depending on the way in which the qubits are built. Since these primitive operations are analogous to logic gates in classical computing, systems built using this approach are called "digital quantum computers". A quantum computer sets up some qubits, applies quantum gates to entangle and manipulate probabilities, then finally measures the outcome, collapsing superpositions to the actual sequence of 0s and 1s.

An easy way to visualize the action of a gate is to visualize qubit as a vector pointing along the surface of the Bloch sphere.

3.5 Commonly used 1,2 and 3 qubit quantum gates:

3.5.1 Pauli X, Y and Z gates: This is basically a bit flip gate, if the qubit is in |0> state, it will rotate along X- axis by 180 degrees to |1>. Similarly, Y and Z gates rotate the qubit by 180 degrees around Y and Z axes respectively.

3.5.2 Hadamard gate: This gate performs rotation around X plus Z axes, takes |0> to the superposition of |0>+|1>. A second hadamard gate rotates it back to |0> state.

3.5.3 CNOT gate: This gate performs conditional rotations on a target qubit depending on the state of a control qubit. Assume q0 is control qubit and q1 is target qubit, if a CNOT is performed between q0 and q1, if q0 is in |0> state nothing happens to q1, if q0 is in |1> state, q1 rotates by 180 degrees.

3.5.4 Toffoli(CCNOT) gate: This gate performs conditional rotations on a target qubit depending on the states of two control qubits. Assume q0 is control qubit and q1 is target qubit, if a CNOT is performed between q0, q1 and q2, if q0 and q2 is in |0> state nothing happens to q1, if q0 and q1 are in |1> state, q2 rotates by 180 degrees. The Toffoli gate is related to the classical AND and XOR operations as it performs the mapping |a,b,c> → |a,b,XOR(c,AND(a,b))>.

3.6 Addition using quantum gates and qubits:

3.6.1 Half adder

As mentioned in section CNOT gate is a controlled rotation gate, here, input |A> is used to control |B>. |A> CNOT |B> immediately gives the output of the B register as

$A \oplus B = S$ which is the sum |S>.

Now a CCNOT gate is used to calculate the carry, this is done using registers A and B as control registers and initialising the third register (C) in state $|0\rangle$, giving the output of the third register as $A \cdot B = C$.

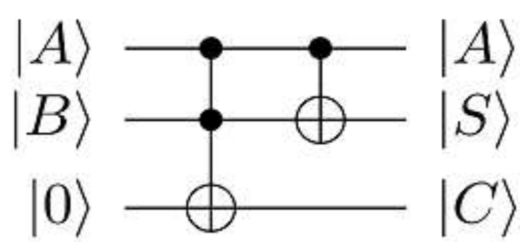

Fig.5 Quantum Half Adder

3.6.2 Full adder

A simple way of doing this for single bits is by using 4 qubit registers, here labelled A, B, Cin and D, where D starts in state |0⟩, so the initial state is : |A⟩|B⟩|Cin⟩|0⟩.

Steps occurring in figure are:

1. Apply Toffoli using A and B to control D:
   |A⟩|B⟩|Cin⟩|A·B⟩
2. CNOT with A controlling B:
   |A⟩|A⊕B⟩|Cin⟩|A·B⟩
3. Toffoli with B and Cin controlling D:
   |A⟩|A⊕B⟩|Cin⟩|A·B⊕(A⊕B)·Cin=Cout⟩
4. CNOT with B controlling Cin:
   |A⟩|A⊕B⟩|A⊕B⊕Cin=S⟩|Cout⟩
5. To get back the inputs A and B is to apply a CNOT with A controlling register B
   |ψout⟩=|A⟩|B⟩|S⟩|Cout⟩

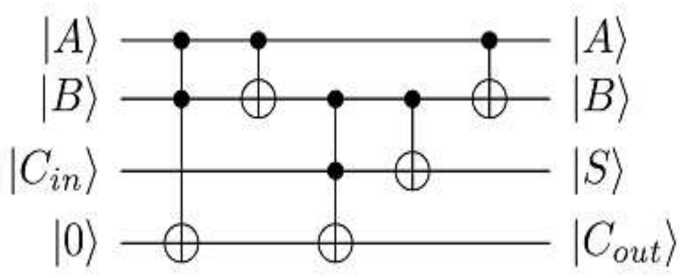

Fig.6 Quantum Full Adder

3.7 Quantum supremacy by google

The tantalizing promise of quantum computers is that they can do certain tasks exponentially faster than classic computers and the quantum supremacy experiment is proof that this is indeed the case. In a world first, a team led by John Martinis, an experimental physicist at the University of California, Santa Barbara, and Google in Mountain View, California, says that its quantum computer carried out a specific calculation that is beyond the practical capabilities of regular, ‘classical’ machines. Google estimates that the same calculation would take even the best classical supercomputer 10,000 years to complete. Although the calculation Google chose checking the outputs from a quantum random-number generator has limited practical applications,the scientific achievement is considered to be huge.

The task Google set for its quantum computer was designed to be extremely difficult for an ordinary computer to solve. The team challenged its computer, known as Sycamore, to describe the likelihood of different outcomes from a quantum version of a random-number generator. They do this by running a circuit that passes 53 qubits through a series of random operations. This generates a 53-digit string of 1s and 0s with a total of 253 possible combinations.

Sycamore calculated the probability distribution by sampling the circuit running it one million times and measuring the observed output strings. The method is similar to rolling the dice to reveal its bias. IBM, a rival to Google in building the world’s best quantum computers, reported in a preprint that the problem could be solved in just 2.5 days using a different classical technique. That paper has not been peer reviewed. If IBM is correct, it would reduce Google’s feat to demonstrating a ‘quantum advantage’ doing a calculation much faster than a classical computer, but not something that is beyond its reach. This would still be a significant landmark.

4. CONCLUSION:

With Google’s Sycamore showing a landmark feat in quantum supremacy, it attracted many more computer scientists to research further into this technology. As we are nearing the tails end of transistor shrinking, either to build quantum computers or to shrink transistors below the size of an atom, we need to dabble in quantum mechanics, so one way or the other quantum physics has a future in the computing industry. It will also give us an opportunity to properly leverage theoretical machine learning and artificial intelligence models on large datasets. Though the future of quantum computers being the sixth generation computers can not be unequivocally stated, the advantages and possibilities they offer can not be denied.

REFERENCES:

[1] Emily Grumbling and Mark Horowitz, Quantum Computing: Progress and prospects, National Academies of Sciences, Engineering, 2019.

[2] Frank Arute, Kunal Arya., Quantum supremacy using a programmable superconducting processor, Nature, 2019.

[3] Elizabeth Gibney, Hello quantum world! Google publishes landmark quantum supremacy claim, Nature, 2019.

[4] Edwin Pednault, John A. Gunnels, Giacomo Nannicini, Lior Horesh, Robert Wisnieff, Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits, arXiv:1910.09534, 2019.

[5] Steve Blank, Things will never be the same for consumer devices, IEEE Spectrum, 2018.