24CS571-QUANTUM COMPUTING

UNIT I – QUANTUM COMPUTING BASICS & MATHEMATICAL FOUNDATIONS

Introduction to Quantum Computing – History and Evolution – Limitations of Classical Computing – Classical vs Quantum Computing – Qubits and Quantum States – Superposition – Entanglement – Bloch Sphere Representation – Quantum Measurement – Applications of Quantum Computing.

Mathematical Foundations: Complex Numbers – Vector Spaces – Linear Algebra – Matrices – Tensor Products – Eigenvalues and Eigenvectors – Dirac Bra-Ket Notation – Principles of Quantum Mechanics – Quantum State Transformations – Introduction to Quantum Programming Environments (IBM Quantum Platform, Qiskit).

Introduction to Quantum Computing

Quantum computing is a modern way of computing that is based on the science of quantum mechanics and its unbelievable phenomena. It is a beautiful combination of physics, mathematics, computer science and information theory. It provides high computational power, less energy consumption and exponential speed over classical computers by controlling the behavior of small physical objects i.e. microscopic particles like atoms, electrons, photons, etc.

Quantum computing is a rapidly-emerging field focused on the development of computer technologies centered on the principles of Quantum Physics. Quantum Physics explains the nature and behaviour of energy and matter on the quantum (atomic and subatomic) scale.
Quantum computing uses a combination of bits to perform specific computational tasks with greater efficiency than their classical counterparts. Even though quantum computers are not going to replace classical computers, quantum technology is significantly changing the way the world operates.

Need for quantum computers

Quantum computers can solve any computational problem that any classical computer can. According to the Church-Turing thesis, the converse is also true that classical computers can solve all the problems of quantum computers too. It means they provide no extra benefit over classical computers in terms of computability but there are some complex and impossible problems that cannot be solved by today's
conventional computers in a practical amount of time. It needs more computational power. Quantum computers can solve such problems in reasonably and exponentially power time complexities, also known as "**Quantum Supremacy**"

Peter Shor in 1993 showed that Quantum computers can help to solve these problems considerably more efficiently like in seconds without getting overheated. He developed algorithms

for factoring large numbers quickly. Since their calculations are based on the probability of an atom's state before it is actually known. These are having the potential to process data in an exponentially huge quantity.

It also explains that a practical quantum computer could break the cryptographic secret codes. It can risk the security of encrypted data and communication. It can expose private and protected secret information. But the advantages of quantum computers are also kept in mind that is significantly more than its flaws. Hence,they are still needed and further research is going towards a brighter future.

Fundamentals of quantum computing

While designing the conventional computer, it was kept in mind that transistors' performance especially when getting smaller, will be affected by noise if any type of quantum phenomenon takes place. They tried to avoid quantum phenomena completely for their circuits. But the quantum computer adapts a different technique instead of using classical bits and even works on the quantum phenomenon itself. It uses quantum bits that are analogous to classical bits and have two quantum states where it can be either 0 or 1 except it follows some quantum properties where it can have both values simultaneously leading to a concept of superposed bits.

History and Evolution

Evolution in one region of science and technology leads to the discovery of a new one. In less than a century, research and development of functional computing technologies have renovated science, technology, and nation massively. The first practical computer around the 20th century was not capable of doing mathematical computations, on its own. Practical devices need a solid physical implementation of theoretical concepts. Nowadays, computers are solving problems instantly

and accurately provided the input is relevant, and a set of instructions given are favorable. It all started from World War II when Alan Turing created a real general purpose computer with a storable program model and is known as the 'Universal Turing Machine'. It was redesigned by Von Neumann and is now the most important architecture for almost every computer. The computers and their physical parts kept improving with time in terms of performance and their strengths. And gradually, the industry of computers became larger than the military department which initiated it. The advancement in control and understanding of humans over nature and physical systems has given us the latest electronic devices we are utilizing today

A new kind of computing

Today's computers are smaller, cheaper, faster, greatly efficient, and even more powerful as compared to early computers that used to be huge, costly, and more power-consuming. It becomes possible due to improvements in architecture,hardware components, and software running on them. Electronic circuits used in computers are getting smaller and smaller day by day.

Transistors are small semiconductor devices that are used to amplify and also switch electric or electronic signals. They were used to be fabricated on a piece of silicon. The circuit was made by connecting these transistors together into a single silicon surface. The shape of circuits in an IC was printed together in all layers of silicon at the same time. This process takes the same amount of time even if the number of transistors in the circuit was increased.

The cost of production of IC was decided by the size of silicon and not the number of transistors. This reduced the price of products due to which manufacturing and selling of IC increased and thus benefits and sales also. From the idea of connecting individual transistors to the collection of these transistors (Logic Gates) and finally, the collection of these Logic Gates used to get connected into a single integrated circuit (IC). Nowadays, a single IC can even integrate small computers onto it. Gordon Moore, co-founder of Intel, in 1965, discovered that the number of transistors on a silicon microprocessor chip had made twice as much every year while the prices were reduced to half since their invention. This is known as Moore's Law. Moore's Law is considerable because it means that computers and their computing power get smaller and faster over time. Though this law is putting the brakes on now and consequently, the improvement in classical computers is not like before it used to be [2].

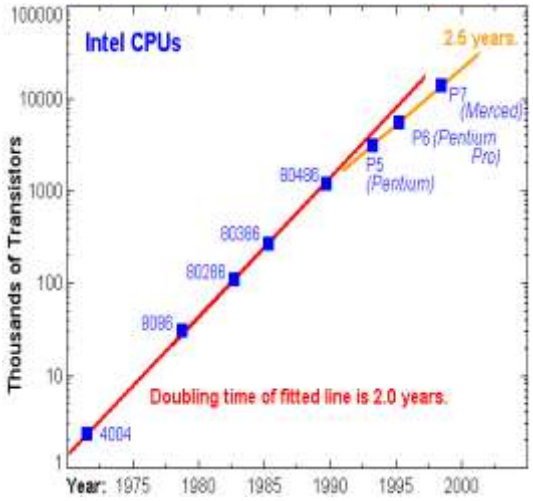
This leads to the idea of the smallest computer by reducing the size of the circuit up to the size of an atom. But then these circuits will not be able to act as a switch as electrons inside an atom can become invisible from one side of a barrier and appear on another side, i.e. they can exist in more than one place at the same time.This is due to the teleporting phenomena in quantum mechanics called "Quantum Tunneling".

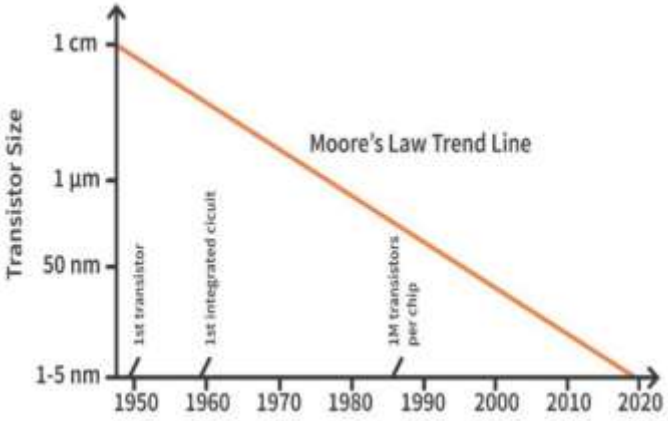
Moore's law & its end

In 1965, Gordon E. Moore—co-founder of Intel—postulated that *"the number of transistors that can be packed into a given unit of space will double about every eighteen months"*. This is also known as Moore's Law

Gordon Moore did not call his observation as "Moore's Law," nor did he set out to create a "law". Moore made this statement based on noticing emerging trends in chip manufacturing at the semiconductor industry. Eventually, Moore's insight became a prediction, which in turn became the golden rule known as Moore's Law.

Moore's Law implies that computers, machines that run on computers, and computing power all become smaller, faster, and cheaper with time, as transistors on integrated circuits become more efficient.





Is Moore's Law Coming to an End?

The electronic industry for computers grows hand-in-hand with the decrease in size of the integrated circuits. This miniaturization is necessary to increase computational power, that is, the number of floating-point operations per second (FLOPS) a computer can perform. In 1950's, electronic computers were capable of performing approximately 103 FLOPS while present supercomputers have a power greater than 1013 FLOPS. According to Moore's law, the number of transistors that may be placed on a single integrated circuit chip doubles approximately every 18 – 24 months. The present limit is approximately **108 transistors** per chip and the typical size of circuit components is of the order of 100 nano meters. That means, we have reached the atomic size for storing a single bit of information and quantum effects have become unavoidably dominant. This is nothing but an end of Moore's law. We need some alternative and is one such alternative is quantum computing.

Quantum computers are based on quantum bits (qubits) and use quantum effects like *superposition* and *entanglement* to their benefit, hence overcoming the miniaturization problems of classical computing.

Classical VS Quantum Computing

Quantum mechanics being a more general model of physics than classical mechanics give rise to a more general model of computing- quantum computing that has more potential to solve problems that cannot be solved by classical ones. To store and manipulate the information, they use their own quantum bits also called '*Qubits*' unlike other classical computers which are based on classical computing that uses binary bits 0 and 1 individually. The computers using such type of computing are known as '*Quantum Computers'*. In such small computers, circuits with transistors, logic gates, and Integrated Circuits are not possible. Hence, it uses the subatomic particles like atoms, electrons, photons, and ions as their bits along with their information of spins and states. They can be superposed and can give more combinations. Therefore, they can run in parallel using memory efficiently and hence is more powerful. Quantum computing is the only model that could disobey the Church-Turing thesis and thus quantum computers can perform exponentially faster than classical computers.

Comparison key	Classical computer	Quantum computer
Basis of computing	Large scale multipurpose computer based on classical physics	High speed computer based on quantum mechanics
Information storage	Bit-based information storage using voltage/charge	Quantum bit-based information storage using electron spin or polarization
Bit values	Bits having a value of either 0 or 1 can have a single value at any instant	Qubits have a value of 0, 1 or sometimes linear combination of both, (a property known as superposition)
Number of possible states	**The number of possible states is 2 which is either 0 or 1**	The number of possible states is infinite since it can hold combinations of 0 or 1 along with some complex information
Output	**Deterministic (repetition of computation on the same input gives the same output)**	Probabilistic (repetition of computation on superposed states gives probabilistic answer)
Gates used for processing	**Logic gates (AND, OR, NOT, etc.)**	Quantum gates (X, Y, Z, H, CNOT etc.)

Operations	**Operations use Boolean Algebra**	Operations use linear algebra and are represented with unitary matrices
Circuit implementation	**Circuit implemented in macroscopic technologies (e.g. CMOS) that are fast and scalable**	Circuits implemented in microscopic technologies (e.g. nuclear magnetic resonance) that are slow and delicate

1. Where the concept of bits came from?

Transistors are the fundamental construction blocks for an IC which are con-nected through wires in a circuit. They conduct electric signals between devices. The communication between transistors within an IC takes place through electric signals.

The behavior of the signals is analog in nature. Therefore, their values are real numbers that change smoothly between 0 and 1. These electric signals can also interact with the environment resulting in noise. Therefore, a little change from 0 to 0.1 due to temperature or vibrations from the environment can drastically change the system's behavior.

There are two types of noise present in the environment. The first type of noise results from energy instabilities occurring suddenly within the object like temperature above absolute zero Kelvin. These are fundamental in nature. Other types of noise are the consequences of signal interactions. This type of noise could have corrected or designed. But neither of them got designed nor corrected or maybe left intentionally uncorrected at the hardware layer. They are systematic in nature [5].

To overcome these noises in analog circuits, the IC is built with transistors in such a way that it could work on digital signals (binary bits) instead of analog signals. These circuits are called 'Logic Gates'. They perceive the electric signals containing values of real numbers as a binary digit or 'bit' of either 0 (low voltage) or 1 (high voltage).

Registers are another type of Gate which stores a bit or the number of bits present in an input value to process further. Gates can remove noise from a signal by limiting the set of values a signal can hold. Constructing IC using logic gates rather than transistors simplifies the designing by creating a powerful circuit that is not sensitive to design and fabrication issues and facilitates abstraction to designers so that they can focus only on gate functions (Boolean functions) rather than circuit issues. Boolean functions are defined by the rules of Boolean algebra.

They can use an automated design tool for mapping the required logic gates. A standard library containing a set of tested logic gates is integrated into the silicon chip

design with the help of their manufacturing technology. Negligible error rates can be achieved using digital logic and standard libraries. This helps in making the design robust. Also, the data is encoded by adding some redundant bits in the memory using an error correction code. This code is checked at regular intervals to detect the error. It also helps in other traits of design like testing and debugging.