Unit – 5: Quantum Computing

***Quantum Computation**: Classical Gates and operations, AND, OR, NAND, XOR Gates and operations. Unitary operations, Pauli Matrices, Quantum Logics: Hadamard, Pauli-X, Y, Z and R, CNOT, Swap Gates and their unitary operations, influence of ECG Sudharshan and GS Agarwal.*

Introduction:

Classical digital computers, which operate on bits as either 0 or 1, are incredibly powerful but face inherent limitations when solving certain complex problems. As technology pushes limits like miniaturization and speed, classical computers confront physical and computational barriers. Some problems—such as simulating quantum systems, optimizing vast combinations, or factoring large numbers—become intractable or would take classical supercomputers thousands of years to solve. Quantum computers leverage the principles of quantum mechanics to overcome these limitations and open new frontiers of computing power.

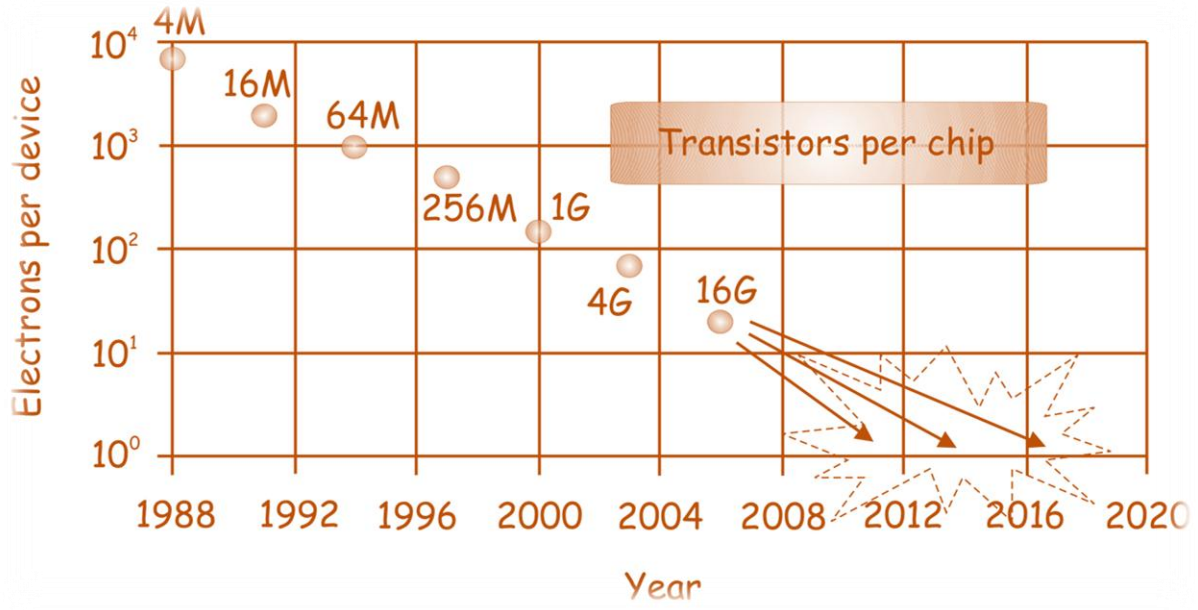
Digital computers process information deterministically using bits, which restricts their ability to represent and explore multiple probabilities simultaneously. This makes them inefficient at solving problems that require exploring many possibilities or complex interactions in parallel. Additionally, classical algorithms often scale poorly, resulting in exponential growth in computation time and power for certain tasks like cryptography, material simulations, and combinatorial optimization.

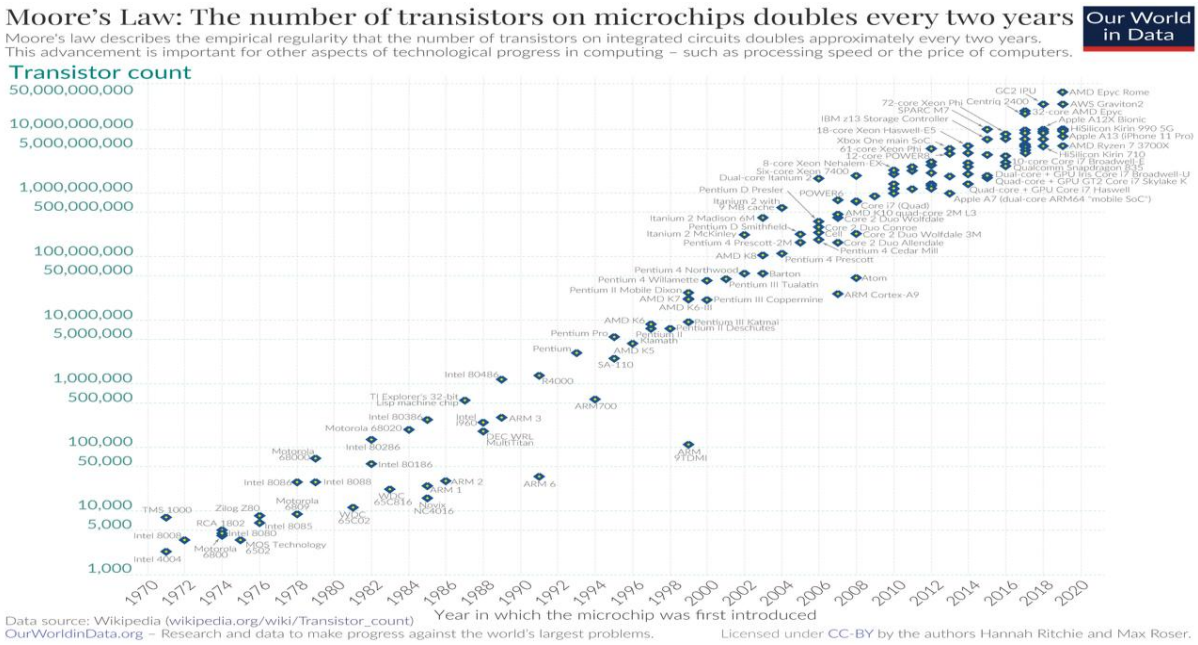
Key limitations of classical digital computers explained simply for students:

- **Limited Processing Power for Complex Problems:** Classical computers use bits as either 0 or 1, which restricts their ability to handle problems requiring simultaneous exploration of many possibilities. This makes tasks like simulating molecules or factoring large numbers very slow or practically impossible.
- **Inability to Handle Exponential Growth of Data:** Many problems grow exponentially in complexity, and classical computers have difficulty scaling efficiently to solve these within reasonable time.
- **Lack of Intuition and Common Sense:** Computers follow precise instructions without understanding context; they cannot make decisions or learn on their own without explicit programming.
- **Deterministic and Sequential Nature:** Classical computers process information in a sequential, deterministic way, limiting their ability to perform massive parallel computation naturally.
- **Physical Limitations:** Issues like heat generation, power consumption, and transistor size limits affect the speed and miniaturization of classical computers.

- **Vulnerability to Errors and Failures:** They can be affected by hardware failures, software bugs, and security vulnerabilities like viruses and hacking.
- **Dependence on Instructions:** They cannot innovate or create new solutions independently but require human input for every task.

These limitations motivate the development of new technologies like quantum computers that can process complex information in fundamentally different ways.





The image presents a graph showing the trend of electrons per device against the increasing number of transistors per chip over time, spanning from 1988 to around 2020.

As the number of transistors per chip grows from 4 million (4M) in 1988 to 16 billion (16G) in later years, the number of electrons required per device drops dramatically. This downward trend, indicated by arrows, reaches nearly single electrons per device by around 2008. The chart demonstrates that as chip technology advances, devices operate with fewer and fewer electrons, highlighting the progression toward physically smaller and more efficient electronic components. Such miniaturization brings classical computation closer to physical and quantum limits, which pose significant challenges for further scaling. This trend is one reason why alternative computing technologies like quantum computing are being explored.

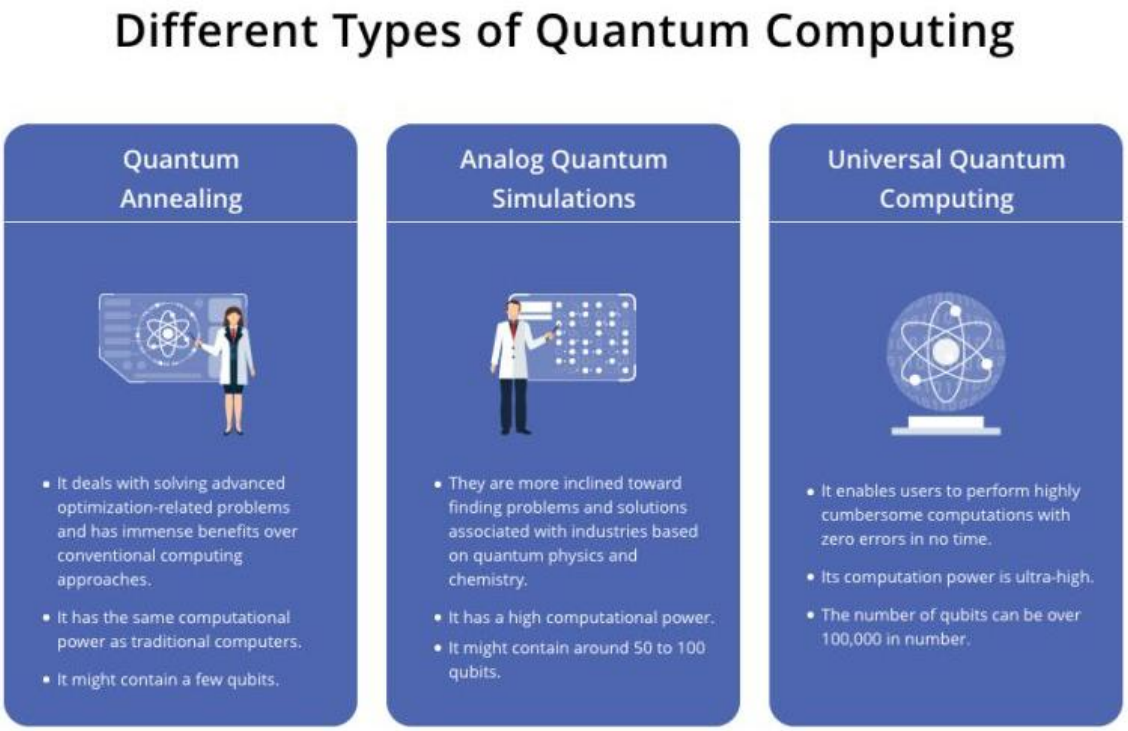
The data exhibited above illustrates theoretical limitation of Moore's Law, which observes that the number of transistors on microchips has doubled approximately every two years from 1970 to 2020. This dramatic growth in transistor count, from just a few thousand to tens of billions, enabled rapid increases in computing power over the decades. The graph displays various processor models, showing a consistent exponential rise in the number of transistors with each new generation of chips. This trend has been a key driver in the advancement of technology, making computers faster, more efficient, and more affordable. However, maintaining Moore's Law has also become increasingly challenging due to physical and engineering limitations as components approach atomic scales. This visualization emphasizes the historical importance of transistor scaling in technological progress and hints at the growing need for new computing paradigms as we approach fundamental limits.

A comparison of Classical and Quantum Computers

Property	Classical Computer	Quantum Computer
States	Defined precisely	Defined using probability functions and are more accurate
Bits	c-bit 0 or 1	q-bit or Qubit 0, 1 and superposition of 0 & 1
Operations	Using two bits only	1 qubit →$\|0\rangle$ or $\|1\rangle$ or $\|0\rangle+\|1\rangle$ or $\|0\rangle-\|1\rangle$ 2 qubit →$\|00\rangle$, $\|11\rangle$, $\|01\rangle$, $\|10\rangle$ and their superposition 3 qubit →$\|000\rangle$, $\|111\rangle$, $\|001\rangle$, $\|010\rangle$, $\|011\rangle$, $\|100\rangle$, $\|101\rangle$, $\|110\rangle$ and their superposition ……. N qubit → $\|00\ldots..0\rangle$ --- $\|11\ldots..1\rangle$ and their suprposition
Operations	Boolean logical	Unitary
Gates	AND, OR, NOT, XOR, NAND, NOR, ..	Hadamard, X, Y, Z, T, C-NOT, Toffoli/CC-NOT, …..
Speed	Limit reached	Unimaginable speed

Classification of Quantum Computers

Quantum computers are generally categorized into three approaches: Quantum Annealer, Analog Quantum, and Universal Quantum computers, each with distinct operational principles and applications.



Quantum Annealer

- Quantum annealing is a specialized quantum computing approach designed for solving optimization problems by finding minimum energy states in complex systems.
- Quantum annealers, such as those built by D-Wave, use quantum fluctuations and adiabatic evolution to quickly explore potential solutions and converge on the "best" answer for problems like scheduling, logistics, or materials design.
- They are efficient and practical for optimization tasks, but cannot run general-purpose quantum algorithms such as Shor's or Grover's.

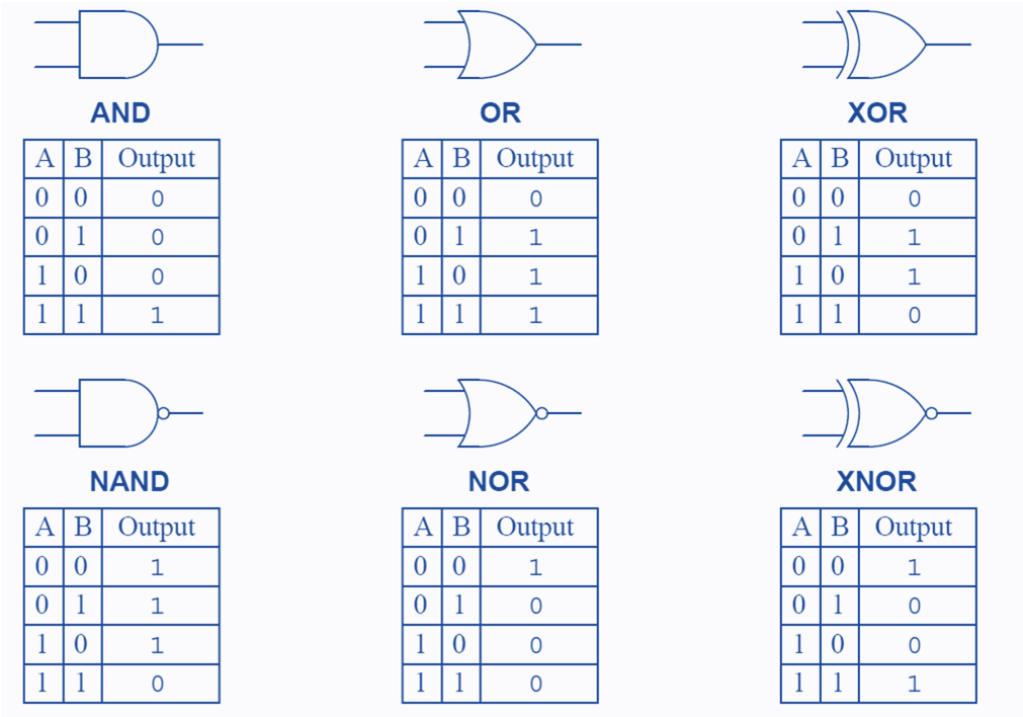
Analog Quantum

- Analog quantum computers simulate quantum systems by directly mapping the problem's parameters onto the behavior of a controlled quantum system.
- This model is ideal for studying quantum physics, chemistry, and material interactions, but lacks the flexibility and universality of gate-based systems.
- Applications include exploring dynamics of molecules, modeling physical systems, and studying quantum phase transitions.

Universal Quantum (Gate-based)

- Universal quantum computers, often called gate-based quantum computers, use sequences of quantum gates to manipulate qubits and implement any quantum algorithm.
- These machines are capable of solving a wide variety of computational problems, from factoring large numbers (Shor's algorithm) to rapid database search (Grover's algorithm) and complex simulations.
- Examples include IBM, Google, and IonQ devices; though extremely powerful, they are still in development due to engineering challenges for large-scale, error-corrected qubits.

Classical Gates and Operations



AND

A	B	Output
0	0	0
0	1	0
1	0	0
1	1	1

OR

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	1

XOR

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

NAND

A	B	Output
0	0	1
0	1	1
1	0	1
1	1	0

NOR

A	B	Output
0	0	1
0	1	0
1	0	0
1	1	0

XNOR

A	B	Output
0	0	1
0	1	0
1	0	0
1	1	1

Questions on Logic Gates (Classic Gates/Digital Gates)

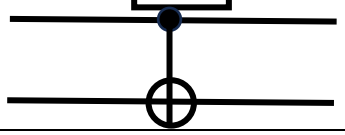
1. Construct a half adder using digital gates
2. Which one is known as universal gate. Construct AND, OR and NOT logic from NAND Gate(s).
3. Convert a single NAND/NOR gate into a NOT GATE.

Unitary Operations, Pauli Matrices

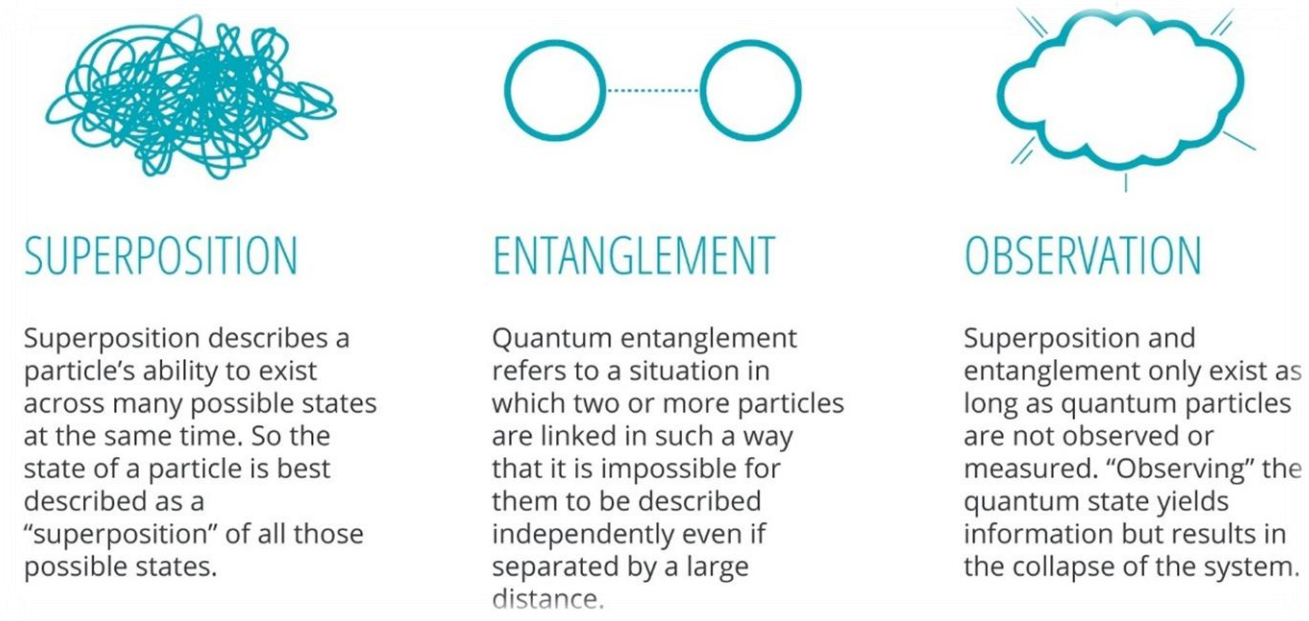
At the end of 19th Century scientists believed that the laws of Physics (which were known at that time) are enough to explain all the events Occur in nature. It was felt that there are

Quantum Logics and Gates

In this course we limit ourselves to one and two-qubit systems only. Also, we will learn to use the Quantum operators corresponding to the single and two-qubit Gates. A summary is shown in the following table:

GATE	SYMBOL	Matrix Operator
X gate (Flip-flop)		$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Y gate (Flip-flop)		$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Z gate		$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Hadamard gate		$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Phase gate		$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$
C-NOT Gate		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
SWAP Gate		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
State	**Symbol**	**Matrix Representation**
0	$\|0\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
1	$\|1\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
00	$\|0\rangle \otimes \|0\rangle = \|00\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
01	$\|0\rangle \otimes \|1\rangle = \|01\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$
10	$\|1\rangle \otimes \|0\rangle = \|10\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$
11	$\|1\rangle \otimes \|1\rangle = \|11\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Three Key concepts in Quantum Computing



1. Superposition

Superposition in quantum computing is a fundamental principle where a quantum bit (qubit) can exist in multiple states simultaneously, rather than being limited to just 0 or 1 like a classical bit.

What Is Superposition?

In classical computing, a bit is always either 0 or 1 at any given moment. In quantum computing, however, a qubit can be in a state represented by any combination (called a linear combination or superposition) of 0 and 1 at the same time. This allows quantum computers to process a vast number of possibilities in parallel and underpins the massive potential speedup in certain quantum algorithms.

Mathematical Representation

A qubit in superposition is typically described mathematically as:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

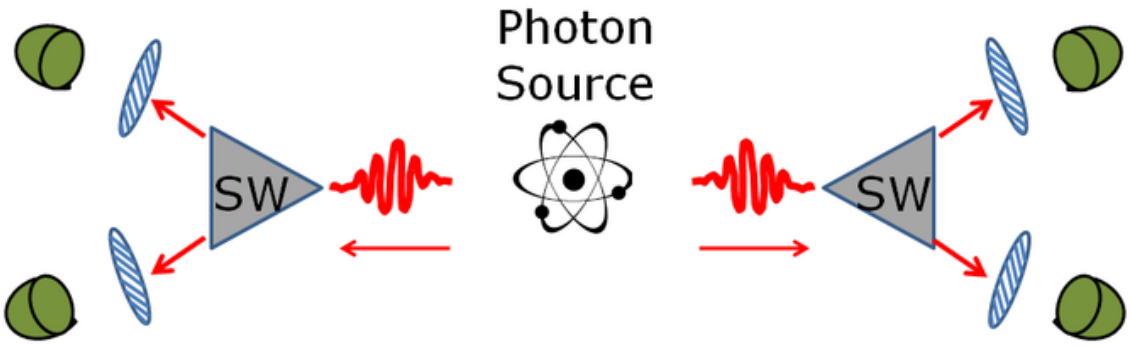
where $|0\rangle$ and $|1\rangle$are the basic states of a single bit quantum computer (similar to 0 and 1 in classical computers), and α and β are complex coefficients called probability amplitudes, which determine the likelihood of measuring the qubit in each state. When you measure a qubit, the superposition "collapses" to either 0 or 1 based on these probabilities. The normalization condition requirement leads to a condition that

$$|\alpha|^2 + |\beta|^2 = 1$$

Why Superposition is Important?

- A single qubit in superposition can encode far more information than a classical bit.
- With n qubits, a quantum computer can represent 2^n different states at the same time—a huge leap in information capacity and parallelism compared to classical bits.
- Superposition, together with quantum entanglement, is what enables quantum computers to solve specific problems much faster than classical computers.

2. Entanglement



Entanglement is a quantum phenomenon in which the quantum states of two or more particles become interconnected such that the state of each particle cannot be described independently of the others, even if they are separated by large distances.

Key Features

- When two particles are entangled, measuring the state of one instantly determines the state of the other, regardless of how far apart they are.
- Entangled systems act as unified ensembles whose full description requires considering all particles together, not individually.
- Entanglement often arises through direct interaction between particles or processes such as spontaneous parametric down-conversion in photons, decay cascades in quantum dots, or other quantum effects.

Importance of Entanglement in quantum computing

- Entanglement is fundamental to quantum mechanics and forms the basis for modern quantum technologies such as quantum computing, quantum cryptography, and quantum teleportation.

- The behavior of entangled particles defies classical explanations and has been experimentally confirmed in many settings, highlighting the nonlocal nature of quantum reality.
- An entangled pair is mathematically represented by a quantum state in the tensor product space of the individual particles' states, which cannot be factored into a product of states of each particle alone. A classic example is the Bell singlet state for two qubits (such as electron spins):

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B\right) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

or equivalently based on electron up an down spins

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A \otimes |\downarrow\rangle_B + |\downarrow\rangle_A \otimes |\uparrow\rangle_B\right) = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle)$$

- Where $|0\rangle$ and $|1\rangle$ (or $|\uparrow\rangle$ and $|\downarrow\rangle$) denote orthonormal basis states of each particle. This superposition state is inseparable, meaning it cannot be written as a simple product like $|\psi\rangle_A \otimes |\phi\rangle_B$ this inseparability is the hallmark of entanglement.
- For example the states defined by $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$ are separable, and it can be written as $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$, hence this is not an entangled state.
- Only the following four pair of states ($|\psi\rangle^+, |\psi\rangle^-, |\phi\rangle^+$ and $|\phi\rangle^-$) are entangled in a two-qubit system.

$$|\psi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \text{ and } |\varphi\rangle^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$

- These pairs are also called as entangled pair, Bell Pair, EPR pair.
- In matrix terms, an entangled state corresponds to a coefficient matrix that has nonzero determinant (or equivalently, cannot be decomposed into rank-1 tensors). The singlet state above exhibits perfect quantum anti-correlation between particle measurements, a key property used in quantum computing protocols.
- This mathematical representation captures how measurement of one particle instantly determines the state of the other, even at a distance, illustrating the nonlocal character of entanglement.
- Thus, entangled pairs are formally represented as specific superpositions in the tensor product Hilbert space of the two particles, fundamentally different from separable classical states

Observation (or Measurement)

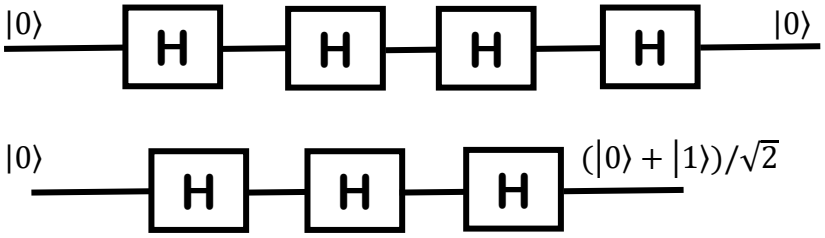
In quantum computing, "measurement" is the process of extracting classical information from a quantum system, typically from qubits. Unlike classical measurement, which simply reveals a pre-existing state, quantum measurement actively changes the system by collapsing the qubit's wavefunction—a superposition of multiple states—into a

definite classical state, usually 0 or 1, with probabilities dictated by the quantum state prior to measurement.

- It is an irreversible process that destroys the superposition and entanglement of measured qubits.
- Measurement outcomes are inherently probabilistic, reflecting the amplitudes in the quantum state.
- Measuring one qubit in a multi-qubit system can affect the overall state due to entanglement.
- Measurements can be done at the end (full-system measurement) or during quantum computation (mid-circuit), enabling conditional operations and error correction.
- Quantum measurement bridges the quantum and classical worlds by translating quantum information into usable classical data for further processing.

Thus, measurement in quantum computing is a critical operation that both reveals and fundamentally alters the quantum state to obtain meaningful classical outcomes from quantum algorithms.

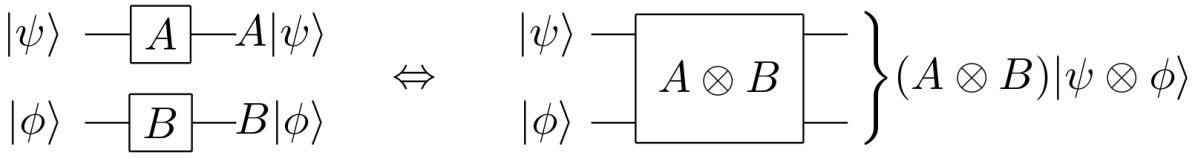
Serial operations of Hadamard Gate:



Serial operations of quantum gates are equivalent to matrix multiplications and does not change the dimensions of the matrix operators.

Parallel operations of Quantum Gates

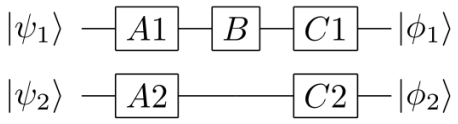
Parallel operations of quantum gates are tensor products, hence change the matrix dimensions. Two Gates *A* and *B* if operated on parallel which is equivalent to *A*⊗*B*.



Solving Quantum Circuits (2-Qubits only)

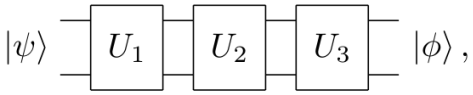
In order to solve a quantum circuit it can be divided into series of unitary matrices and shall be operated from the left side to right side.

Solve the following:



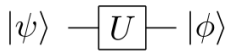
SOLUTION

Step 1:



where $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, $U_1 = A_1 \otimes A_2$, $U_2 = B \otimes I$, $U_3 = C_1 \otimes C_2$ and $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$. Do note that for U_2, it is assumed that a straight connecting line is equivalent to an Identity matrix operation. It is further simplified as

Step 2:



Here $U = U_3U_2U_1$.

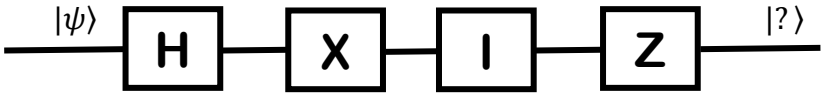
Step 3: Find the output states from the following

$$|\phi\rangle = U\,|\psi\rangle\,.$$

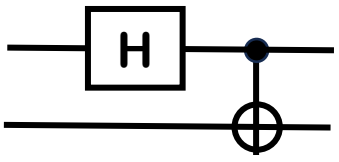
Now, decompose $|\phi_1\rangle$ and $|\phi_2\rangle$ from $|\phi\rangle$ and report.

Sample Questions on Quantum Computing

1. If $|\psi\rangle = |0\rangle$, find H$|\psi\rangle$, X$|\psi\rangle$ and Z$|\psi\rangle$.
2. If $|\psi\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, find H$|\psi\rangle$, X$|\psi\rangle$ and Z$|\psi\rangle$.
3. Using unitary matrices, estimate the following: $H \otimes Z$, $X \otimes Z$ and $H \otimes H$.
4. Show that $H = \frac{X+Z}{\sqrt{2}}$.
5. Find the output of the following,
   if $(i)\ |\psi\rangle = |0\rangle$, $(ii)\ |\psi\rangle = |0\rangle + |1\rangle$ and $(iii)\ |\psi\rangle = |1\rangle$



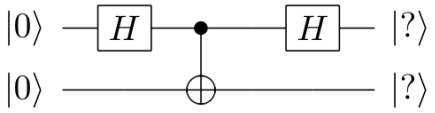
6. What are entangled pair? How to generate it?
7. Show that for all possible inputs, the quantum circuit shown here produces an entangled pair (or Bell pair).



8. Show that a SWAP gate can be composed from $SWAP = \frac{I\otimes I + X\otimes X + Y\otimes Y + Z\otimes Z}{2}$

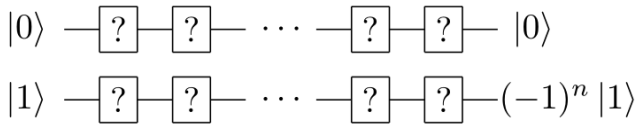
9. Find $|?\rangle$ In the following circuits.

(9a): Find $|??\rangle$

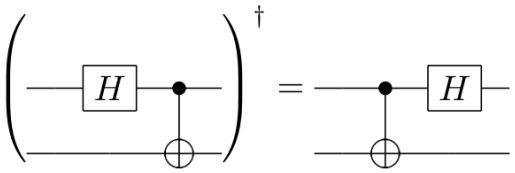


(9b): If a Gate is connected in series for four times, the input state remains unchanged as shown below. Find all Quantum Gates which satisfies the following quantum circuit,

(9c): If a Gate is connected in series for any number of times, the input state statisfies the following. Find all Quantum Gates which satisfies both the quantum circuits shown below,



(9d) Using matrix method show that:



___END of QC___