MODULE-3

Quantum Computing

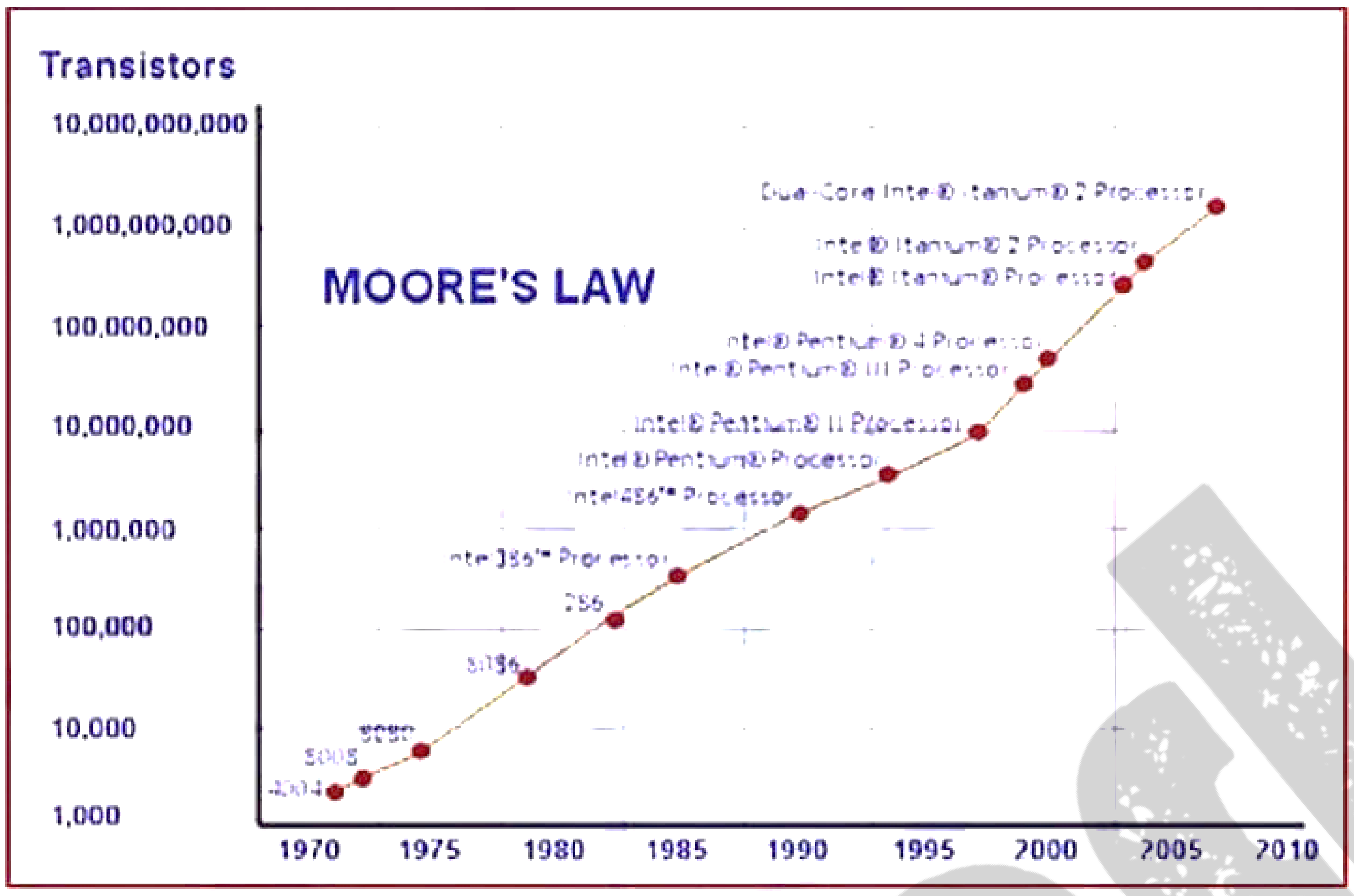
Introduction to Quantum Computing

Quantum Computing is the area of study focused on developing computing methods based on the principle of quantum theory. Quantum computing is based on the principle of quantum superposition. In Quantum computing, the information is encoded in quantum system such as atoms, ions or quantum dots. One quantum rule in particular creates enormous incentives to apply quantum mechanics to computing. The algorithms are also written based on quantum principles in which, Shor's algorithm for factorization and Grover's search algorithm are basics. (Grover is an Indian born Physicist working in Bell Labs). The process of computation is incredibly fast but it has to be done by the help of quantum computers which are yet to be realized in practice. It is expected that 140 digit log number could be factored a billion (109) times faster than classical computation. It is so powerful that a search engine can search every part of internet in half an hour.

Moore's law & its End

In the year 1965, Gordon Moore observed increasing performance in the first few generations of the integratedcircuit (IC) technology. Moore predicted that it would continue to improve at an exponential rate with the performance per unit cost increasing by a factor or two every 18 months are so. The computer industry has followed this prediction since then. But actually the doubling was occurring in every 24 months or 2 years. The following plot shows the 50 years of Moore's law. The question that arises is how long can Moore's law continues to hold and what are the ultimate limitations?. According to the semiconductor size data the size has reached 5 nanometer in 2021. The Demise of the Transistor in the quantum scale could be expected as the dimensions decrease further. Quantum effects can cascade it he micro scale realm causing problems for current microelectronics. The most typical effects are Electron tunneling among the circuit lines. Thus Quantum Computation is the option for the further generation.

Statement: "The number of transistors on a microchip doubles every year"



Differences Between Classical and Quantum Computing

Classical computing	Quantum computing
It is large scale integrated multi-purpose computer.	It is high speed parallel computer based on quantum mechanics.
Information storage is bit based on voltage or charge etc.	Information storage is Quantum bit based on direction of an electron spin.
Information processing is carried out by logic gates e.g. NOT, AND, OR etc.	Information processing is carried out by Quantum logic gates.
Classical computers use binary codes i.e. bits 0 or 1 to represent information.	Quantum computers use Qubits i.e. 0, 1 and both of them simultaneously to run machines faster.
Operations are defined by Boolean Algebra.	Operations are defined by linear algebra over Hilbert Space and can be represented by unitary matrices with complex elements.
Circuit behaviour is governed by classical physics.	Circuit behavior is governed explicitly by quantum mechanics.

Concept of Qubit and its properties

Quantum bits, called qubits are similar to bits having two measurable states called 0 and 1 states. Qubits can also be in a superposition state of these 0 and 1 states as shown in the figure. A qubit can be in a superposition of both 0 and 1. Qubits can be expressed in quantum mechanical states with mathematical formula, Dirac or "brac–ket" notation is commonly used in quantum mechanics and quantum computing. The state of a qubit is enclosed in the right half of an angled bracket, called the "ket". A qubit $|\psi\rangle$ could be in $|0\rangle$ or $|1\rangle$ state which is the superposition of both $|0\rangle$ and $|1\rangle$ state.

This is written as, $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

Where α and β called the amplitude of the states which are a complex number.

Properties of Qubits

Qubit is a basic unit in which of information in a quantum computer. Superposition, Entanglement, and Tunneling are all special properties that define a qubit.

i) A qubit can be in a superposed state of the two states 0 and 1.
Qubit is a superposition of both $|0\rangle$ and $|1\rangle$ state is given by
$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

ii) If measurements are carried out with a qubit in superposed state then the results that we get will be probabilistic unlike how it's deterministic in a classical computer.
The total probability of all the states of the quantum system must be 100%.
i.e. $|\alpha|^2 + |\beta|^2 = 1$ is called Normalization rule.

iii) Owing to the quantum nature, the qubit changes its state at once when subjected to measurement. This means, one cannot copy information from qubits the way we do in the present computers and is known as "no cloning principle".

A Qubit can be physically implemented by the two states of an electron or horizontal and vertical polarizations of photons as $|\downarrow\rangle$ and $|\uparrow\rangle$.

Representation of qubit by Bloch Sphere

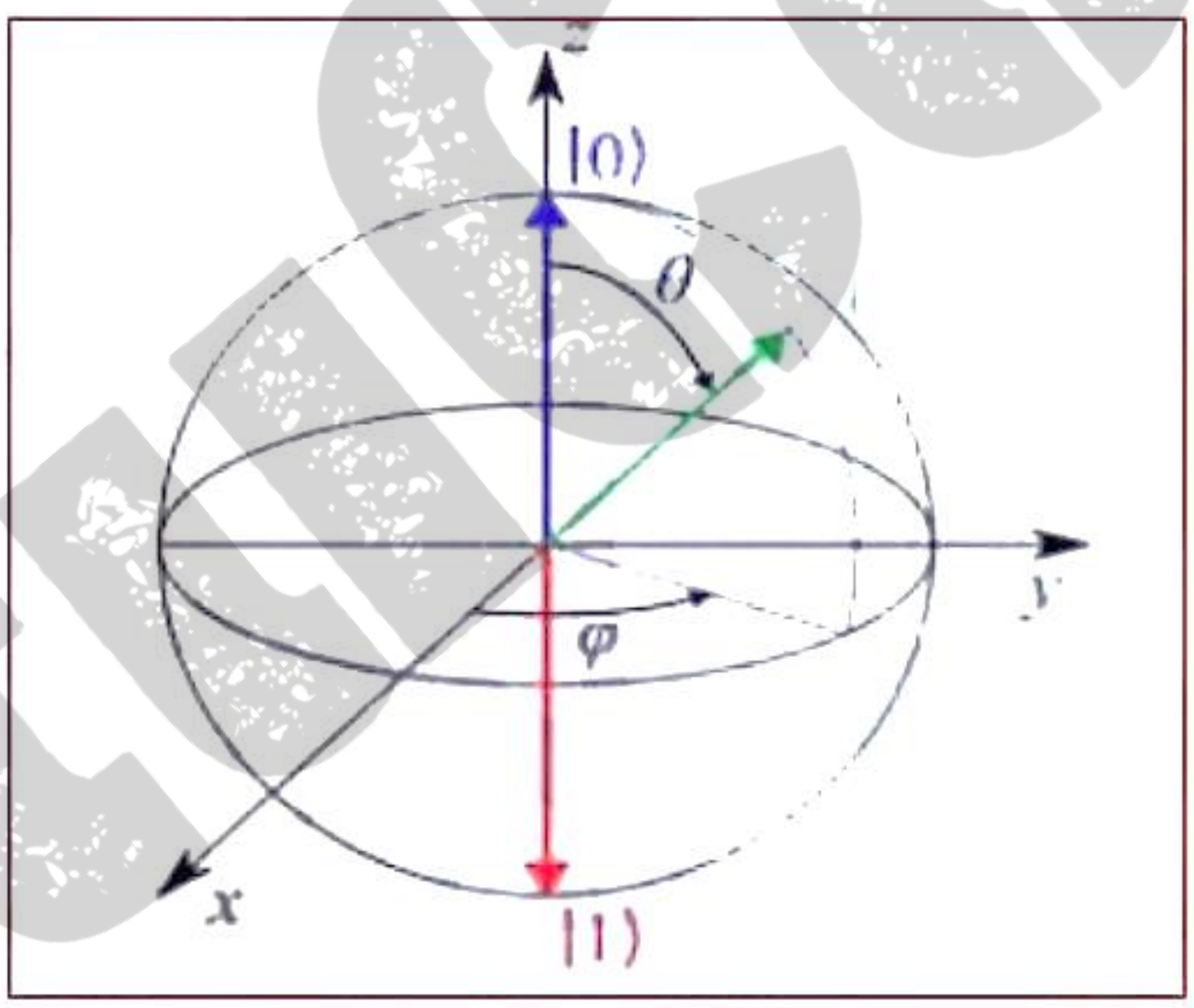
The pure state space qubits (Two Level Quantum Mechanical Systems) can be visualized using an imaginary sphere called Bloch Sphere. It has a unit radius.

The Arrow on the sphere represents the state of the Qubit. The north and south poles are used to represent the basis states $|0\rangle$ and $|1\rangle$ respectively. The other locations are the superposition of $|0\rangle$ and $|1\rangle$ states and represented by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$.

Thus a Qubit can be any point on the Bloch Sphere. The Bloch sphere allows the state of the qubit to be represented unit spherical co-ordinates. They are the polar angle θ and the azimuth angle ϕ.

The Bloch sphere is represented by the equation

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$



Case i) For φ =0 and θ=0 then $|\psi\rangle = |0\rangle$ which is along +z axis.

Case ii) For φ=0 and θ = 180 then $|\psi\rangle = |1\rangle$ which is along -z axis.

Case iii) For φ =0 and θ= $\frac{\pi}{2}$ *then* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ which is along +X axis.

Case iv) For φ =0 and θ= $-\frac{\pi}{2}$ *then* $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ which is along -X axis.

Single and Two qubits and Extension to N qubits

i) Single qubit

A Single qubit has two computational basis states $|0\rangle$ and $|1\rangle$. It is in general written as by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Such that $|\alpha|^2 + |\beta|^2 = 1$

The matrix representation of $|0\rangle$ and $|1\rangle$ is given by

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad and \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

ii) Two qubit

A two qubit system has four computational basis states denoted has $|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$. The two qubit state is given by $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle + \cdots$

iii) N qubit

A multi-qubit system of N qubits has 2^N computational basis states. For example a state of 3 qubits has 2^3 computational basis states. Thus for N-qubit the computational basis states are denoted has $|000\ldots\ldots00\rangle$ $|000\ldots..01\rangle$ $|10\ldots\ldots.00\rangle$ $|10\ldots\ldots.01\rangle$.

Dirac Representation and Matrix Operations

Matrix representation of $|0\rangle$ and $|1\rangle$

The wave function could be expressed in ket notation as $|\psi\rangle$ (ket Vector), ψ is the wave function. The quantum state is given by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and in matrix form $|\psi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$. The matrix form of the states $|0\rangle$ and $|1\rangle$ is given by

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad and \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

Identity Operator

The operator of type $I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$ is called identity operator. When an identity operator acts on a state vector its keeps the state intact. By analogy we study identity operator as an identity matrix.

Let us consider the operation of Identity operator on $|0\rangle$ and $|1\rangle$states. As per the principle of identity operation $I\,|0\rangle = |0\rangle$ and $I\,|1\rangle = |1\rangle$.

$$I\,|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$I\,|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Thus the operation of identity matrix (operator) on $|0\rangle$ and $|1\rangle$states leaves the states unchanged.

Pauli Matrices

Pauli Matrices are set of 2×2 matrices. Which are very much useful in the study of quantum computation and quantum information. The pauli matrices are given by

$$\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad , \; \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \text{and} \;\; \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Pauli Matrices operating on $|0\rangle$ and $|1\rangle$ States

1. $\sigma_x|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

   $\sigma_x|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

2. $\sigma_y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle$

   $\sigma_x|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle$

3. $\sigma_z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

   $\sigma_z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle$

Conjugate of a Matrix

- It is possible to find the conjugate for a given matrix by replacing each element of the matrix with its complex conjugate.
- The conjugate of a complex number is found by switching the sign of the imaginary part.
- The complex conjugate of 1 is just 1 and the complex conjugate of +i is −i.

$$A = \begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix}$$

The conjugate of matrix A is

$$A^* = \begin{bmatrix} 1 & -i \\ 1 & -i \end{bmatrix}$$

Transpose of a matrix

Transpose of a matrix, switches rows with columns.

- The first row turns into the first column, second row turns into the second column.

$$A = \begin{bmatrix} 1 & i \\ 1 & i \end{bmatrix}$$

- The conjugate of matrix A is

$$A^* = \begin{bmatrix} 1 & -i \\ 1 & -i \end{bmatrix}$$

$$A^+ = \begin{bmatrix} 1 & 1 \\ -i & -i \end{bmatrix}$$

Unitary Matrix (U)

- A matrix U is unitary, if the matrix product of U and its conjugate transpose U † (called U-dagger) produces the identity matrix.

$UU^\dagger = U^\dagger U = I = 1$

Let $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Conjugate of U is $U^* = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Transpose of U is $U^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$UU^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I$$

$$U^\dagger U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = I$$

$$UU^\dagger = I$$

Row and Column matrix (Inner product)

- A Row matrix is a vector represented by Brac vector . < |
- A Column matrix is a vector represented by ket vector | >

then $|\psi\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}$; Row vector $|\psi\rangle = [\alpha_1, \beta_1]$,Where Bra vector is a complex conjugate of ket vector.

$$|\psi *\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}$$

$$|\psi\rangle^\dagger = [\alpha_1{}^*, \beta_1{}^*]$$

Thus Brac is the complex conjugate of ket and conversely ket is the complex conjugate of Brac.

Orthogonality and Orthonormal

Two states $|\psi\rangle$ and $|\phi\rangle$ are said to be orthogonal if their inner product is Zero.

Mathematically $\langle\psi|\phi\rangle = 0$

The two states are orthogonal means they are mutually exclusive. Like Spin Up and Spin Down of an electron.

Consider the inner product of and $\langle 0|1\rangle = [1, 0]\begin{bmatrix} 1 \\ 0 \end{bmatrix} = [0 + 0] = 0$

Two states $|\psi\rangle$ and $|\phi\rangle$ are said to be orthonormal if their inner product is one.

Mathematically $\langle\psi|\phi\rangle = 1$

Quantum Gates

In quantum computing a quantum logic gate is a basic quantum circuit operating on a small number of qubits. A qubit is useless unless it is used to carry out a quantum calculation. The quantum calculations are achieved by performing a series of fundamental operations, known as quantum logic gates. They are the building blocks of quantum circuits similar to the classical logic gates in conventional digital circuits.

Quantum Not Gate:

In Quantum Computing the quantum NOT gate for qubits takes the state $|0\rangle$ to $|1\rangle$ and vice versa. It is analogous to the classical not gate. The Matrix representation of Quantum Not Gate is given by $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

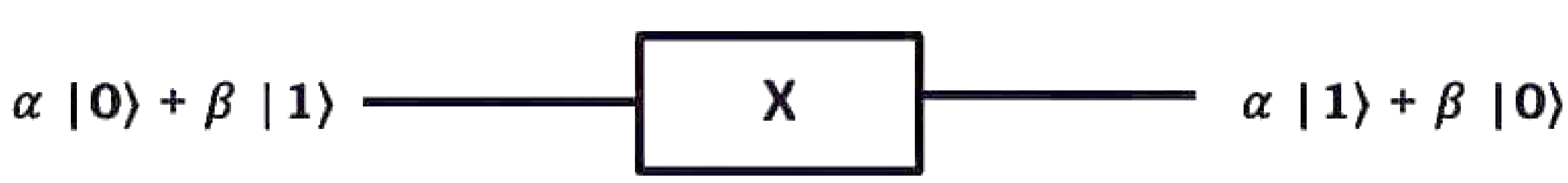
$$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

A Quantum State is given by $\alpha\ |0\rangle + \beta\ |1\rangle$ and its matrix representation is given by $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$

Hence the operation of Quantum Not Gate on quantum state is given by

$$X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

Thus the quantum state becomes $\alpha\ |1\rangle + \beta\ |0\rangle$. Similarly, The input $\alpha\ |1\rangle + \beta\ |0\rangle$ to the quantum not gates changes the state to $\alpha\ |0\rangle + \beta\ |1\rangle$. The quantum not gate circuit and the truth table are as shown below



Quantum Not Gate

Truth table of Quantum Not Gate

Input	Output
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\alpha\ \|0\rangle + \beta\ \|1\rangle$	$\alpha\ \|1\rangle + \beta\ \|0\rangle$

Pauli-X,Y and Z Gates

i) Pauli X Gate

The Pauli-X Gate is nothing but Quantum Not Gate.

ii) Pauli Y Gate

Pauli Y Gate is represented by Pauli matrix σ_y or Y. This gate Maps $|0\rangle$ state to $i\ |1\rangle$ state and $|1\rangle$ state to $-i\ |0\rangle$ state. The Y Gate and its operation is as given below

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle$$

$$Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle$$

Thus the Y-Gate defines the transformation

$$Y\ (\alpha\ |0\rangle + \beta\ |1\rangle) = \alpha Y\ |0\rangle + \beta Y\ |1\rangle = -i\beta\ |0\rangle + i\alpha\ |1\rangle$$

Quantum Y-Gate is represented by

Quantum Y Gate

Truth table of Quantum Y Gate

Input	Output
$\|0\rangle$	$i\|1\rangle$
$\|1\rangle$	$-i\|0\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$-i\beta\|0\rangle + i\alpha\|1\rangle$

iii) Pauli Z Gate

The Z-gate is represented by Pauli Matrix   or Z. Z Gate maps input state $|k\rangle$ to $(-1)|k\rangle$.

1. For input $|0\rangle$ the output remains unchanged.

2. For input $|1\rangle$ the output is $-|1\rangle$.

The Matrix representation and the operation of Z-Gate on $|0\rangle$ and $|1\rangle$ are as follows

$$Z|0\rangle = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

$$Z|1\rangle = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\-1\end{bmatrix} = -|1\rangle$$

$$(\alpha|0\rangle + \beta|1\rangle) = \alpha Z|0\rangle + \beta Z|1\rangle = \alpha|0\rangle - \beta|1\rangle$$

The circuit symbol and the truth table of Z-Gate are as follows

Truth table of Quantum Z Gate

Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$

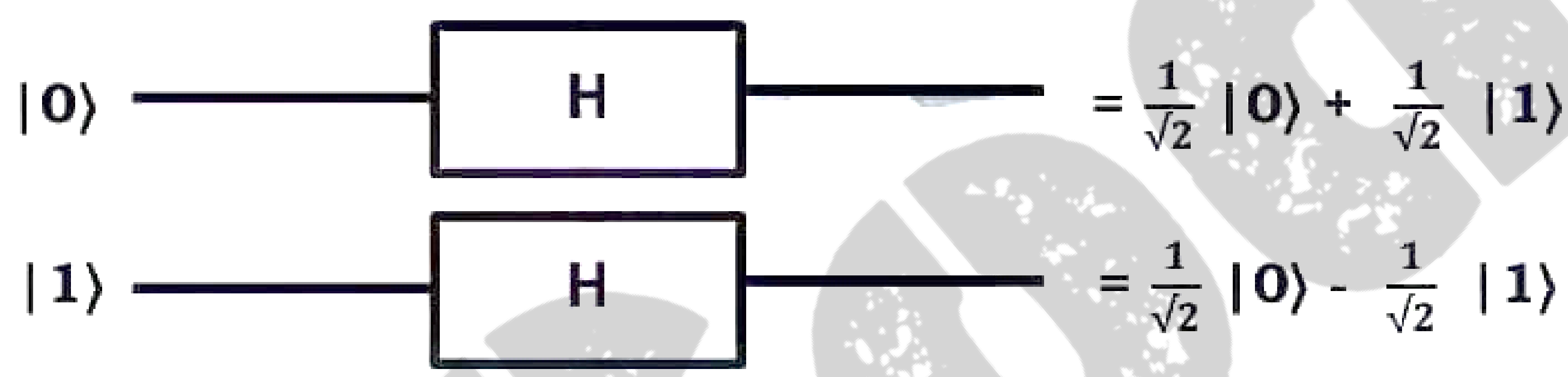
Hadamard Gate

The Hadamard Gate is a truly quantum gate and is one of the most important in Quantum Computing. It is has similar characteristics of $\sqrt{NOT}$ Gate. It is a self-inverse gate. It is used to create the superposition of $|0\rangle$ and $|1\rangle$ states.

The Matrix representation of Hadamard Gate is as follows $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

The Hadamard Gate and the output states for the $|0\rangle$ and $|1\rangle$ input states are represented as follows.

The Hadamard Gate satisfies Unitary Condition. $H^{\dagger}H = I$



The truth-table for the Hadamard Gate is as follows.

Input	Output
$\vert 0\rangle$	$\frac{\vert 0\rangle + \vert 1\rangle}{\sqrt{2}}$
$\vert 1\rangle$	$\frac{\vert 0\rangle - \vert 1\rangle}{\sqrt{2}}$
$\alpha\vert 0\rangle + \beta\vert 1\rangle$	$\alpha\frac{\vert 0\rangle + \vert 1\rangle}{\sqrt{2}} + \beta\frac{\vert 0\rangle - \vert 1\rangle}{\sqrt{2}}$

Phase Gate or S Gate

The phase gate turns a $|0\rangle$ into $|0\rangle$ and a $|1\rangle$ into $i\ |1\rangle$.

The Matrix representation of the S gate is given by

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

The effect of S gate on input $|0\rangle$ is given by

$$S\,|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

Similarly the effect of S gate on input $|1\rangle$ is given by

$$S|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle$$

The transformation of state $|\psi\rangle$ is given by

$$S\ |\psi\rangle = S\,(\alpha\ |0\rangle + \beta\ |1\rangle) = \alpha S\ |0\rangle + \beta S\ |1\rangle = \alpha\ |0\rangle + i\beta\ |1\rangle$$

The symbol of S gate is given by

The Truth table for S gate is as follows

Input	Output
$|0\rangle$	$|0\rangle$
$|1\rangle$	$i|1\rangle$
$\alpha\ |0\rangle + \beta\ |1\rangle$	$\alpha\ |0\rangle + i\ \beta|1\rangle$

T -Gate / $\frac{\pi}{8}$ Gate

The T Gate is represented by the matrix as follows

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix}$$

The Operation of T- gate on $|0\rangle$ and $|1\rangle$ are given by

$$T|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$T|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{1+i}{\sqrt{2}} \end{bmatrix} = \frac{1+i}{\sqrt{2}}|1\rangle$$

T -Gate is also called $\frac{\pi}{8}$ Gate is shown below

$$T = e^{\frac{i\pi}{8}} \begin{bmatrix} e^{-\frac{i\pi}{8}} & 0 \\ 0 & e^{\frac{i\pi}{8}} \end{bmatrix}$$

The symbolic representation of T-gate is given by

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

$\alpha|0\rangle + \frac{1+i}{\sqrt{2}}\beta|1\rangle$

The Truth table for T- gate is as follows

Input	Output
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\frac{1+i}{\sqrt{2}}\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + \frac{1+i}{\sqrt{2}}\beta\|1\rangle$

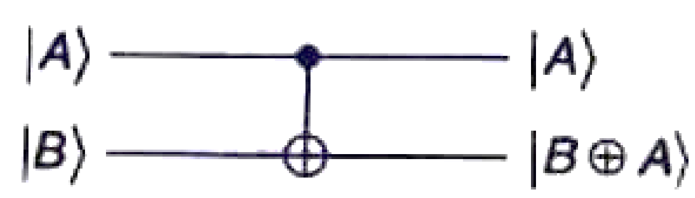
Note: Important feature of T- gate is it could be related to S gate as $T^2 = S$

Multiple Qubit Gates

Multiple Qubit Gates operates on two or more input Qubits. Usually one of them is a control qubit. Controlled Gates 'A' Gate with operation of kind "If 'A' is True then do 'B'" is called Controlled Gate. The $|A\rangle$ Qubit is called control qubit and $|B\rangle$ is the Target qubit. The target qubit is altered only when the control qubit is $|1\rangle$. The control qubit remains unaltered during the transformations.

Controlled Not Gate or CNOT Gate

The CNOT gate is a typical multi-qubit logic gate and the circuit is as follows.



CNOT gate

The matrix representation of CNOT gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The Transformation could be expressed as $|A, B\rangle \rightarrow |A, B \oplus A\rangle$

Consider the operations of CNOT gate on the four inputs $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$.

Operation of CNOT Gate for input $|00\rangle$

Here in the inputs to the CNOT Gate the control qubit is $|0\rangle$. Hence no change in the state of Target qubit $|0\rangle$. $|00\rangle \rightarrow |00\rangle$

Operation of CNOT Gate for input $|01\rangle$

Here in the inputs to the CNOT Gate the control qubit is $|0\rangle$. Hence no change in the state of Target qubit $|1\rangle$. $|01\rangle \rightarrow |01\rangle$

Operation of CNOT Gate for input $|10\rangle$

Here in the inputs to the CNOT Gate the control qubit is $|1\rangle$. Hence the state of Target qubit flips from $|0\rangle$ to $|1\rangle$. $|10\rangle \rightarrow |11\rangle$

Operation of CNOT Gate for input $|11\rangle$

Here in the inputs to the CNOT Gate the control qubit is $|1\rangle$. Hence the state of Target qubit flips from $|1\rangle$ to $|0\rangle$. $|11\rangle \rightarrow |10\rangle$

The Truth Table of operation of CNOT gate is as follows.

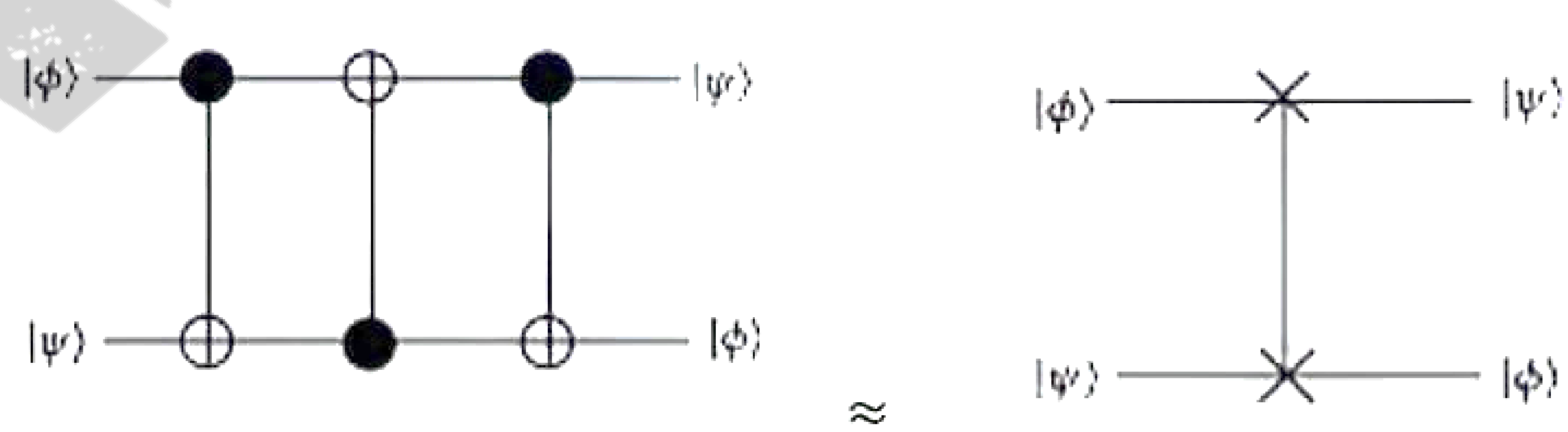
Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

Swap Gate

The SWAP gate is two-qubit operation. Expressed in basis states, the SWAP gate swaps the state of the two qubits involved in the operation. The Matrix representation of the Swap Gate is as follows

$$U_{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

The schematic symbol of swap gate circuit is as follows



The swap gate is a combined circuit of 3 CNOT gates and the overall effect is that two input qubits are swapped at the output. The Action and truth table of the swap gate is as follows.

Truth table of SWAP gate

Input	*Output*
$\vert 00\rangle$	$\vert 00\rangle$
$\vert 01\rangle$	$\vert 10\rangle$
$\vert 10\rangle$	$\vert 01\rangle$
$\vert 11\rangle$	$\vert 11\rangle$

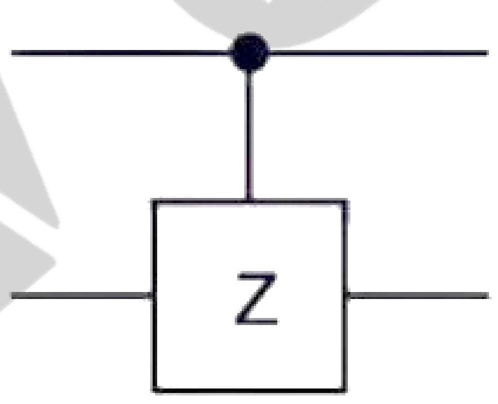
Controlled Z Gate

In Controlled Z Gate, The operation of Z Gate is controlled by a Control Qubit. If the control Qubit is $|A\rangle$ is equal to $|1\rangle$ then only the Z gate transforms the Target Qubit $|B\rangle$ as per the Pauli-Z operation.

The action of Controlled Z-Gate could is specified by a matrix as follows.

$$U_Z = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

The schematic circuit of controlled Z gate and the truth table are as follows



Input	Output
$\vert 00\rangle$	$\vert 00\rangle$
$\vert 01\rangle$	$\vert 01\rangle$
$\vert 10\rangle$	$\vert 10\rangle$
$\vert 11\rangle$	$-\vert 11\rangle$

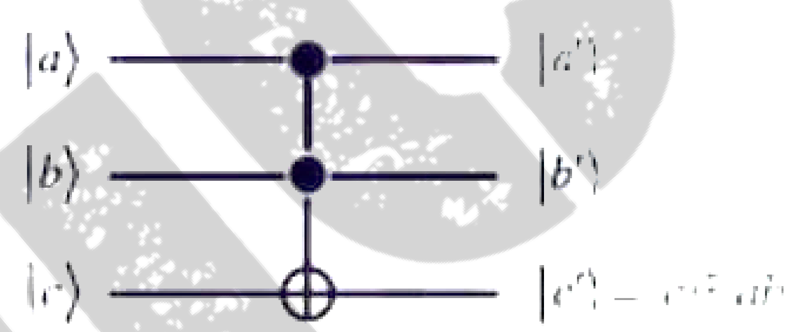
Toffoli Gate

The Toffoli Gate is also known as CCNOT Gate (Controlled-Controlled-Not). It has three inputs out of which two are Control Qubits and one is the Target Qubit. The Target Qubit flips only when both the Control Qubits are |1⟩. The two Control Qubits are not altered during the operation.

The matrix representation of Toffoli Gate is given by

$$U_T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

The schematic circuit of Toffoli Gate is as follows



The truth table for Toffoli gate is as follows

Inputs			Ouputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

The Toffolli matrix is unitary. The Toffolli Gate is its own inverse. It could be used for NAND Gate Simulation.