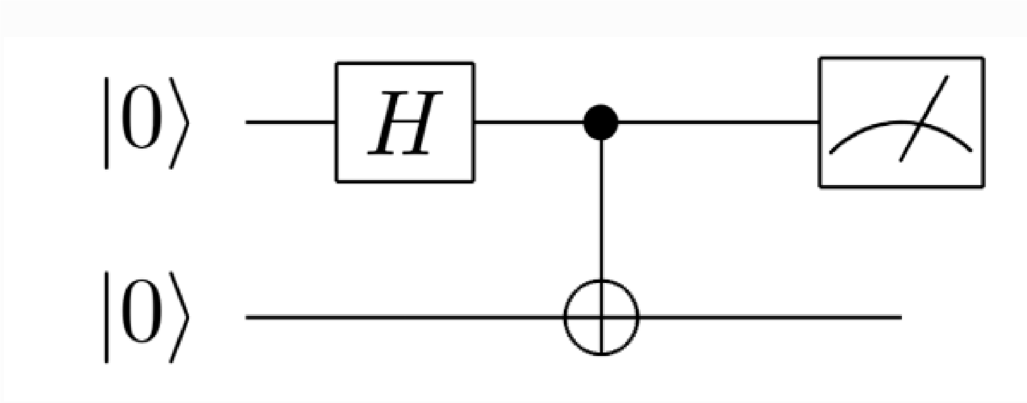
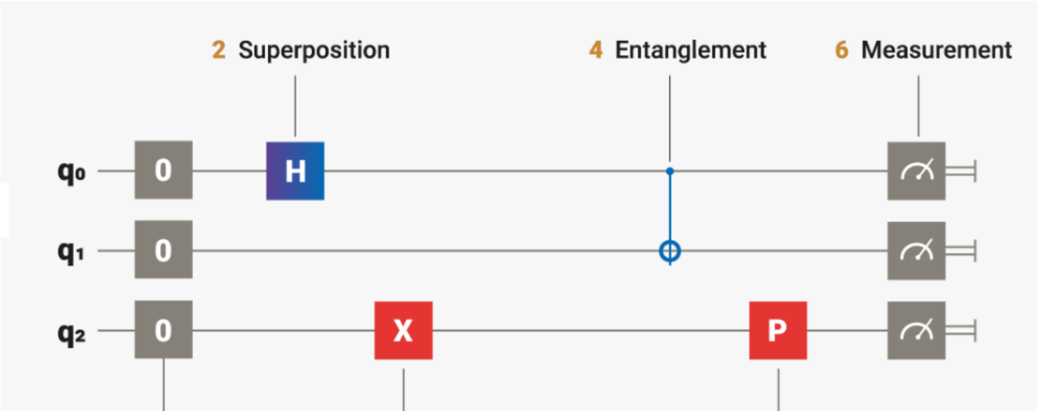
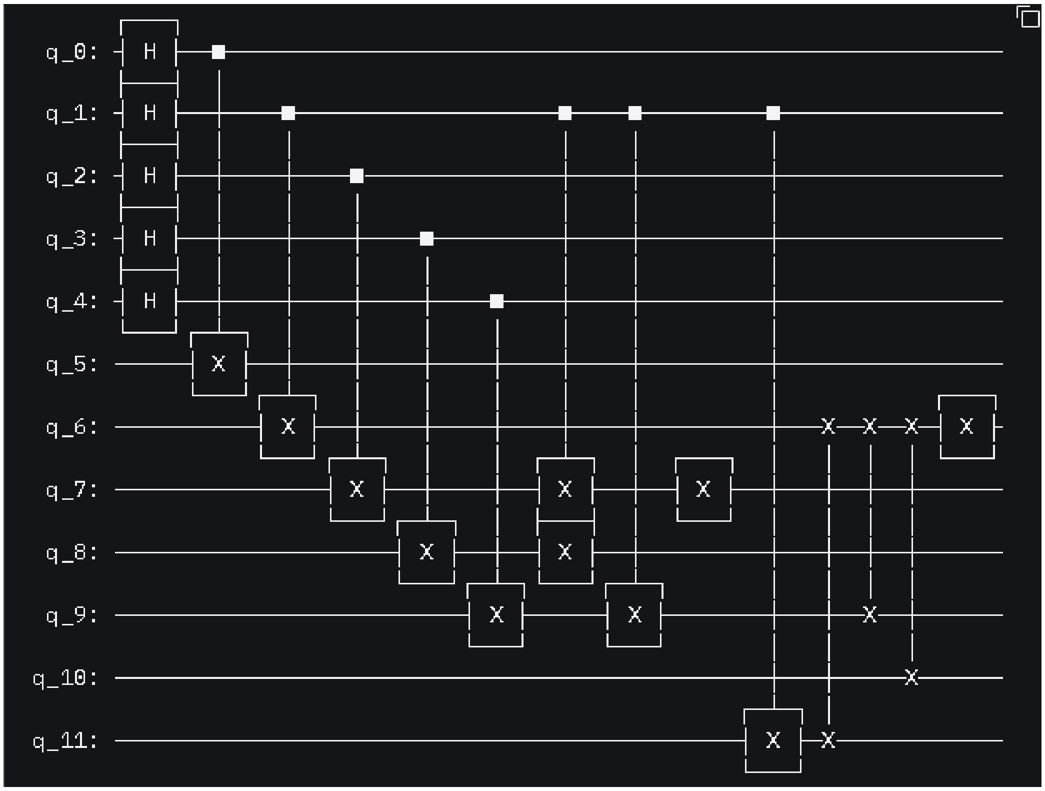
IBM Qiskit Workshop
Fundamentals of Quantum Computing

Speaker: Shahzaib Abbas (University of Karachi)

IBA University (Main Campus)


|0⟩
|0⟩
H


2 Superposition
4 Entanglement
6 Measurement
q0
q1
q2
0
0
0
H
X
P


q_0:
q_1:
q_2:
q_3:
q_4:
q_5:
q_6:
q_7:
q_8:
q_9:
q_10:
q_11:
H
H
H
H
H
X
X
X
X
X
X
X
X
X
X
X

Introduction

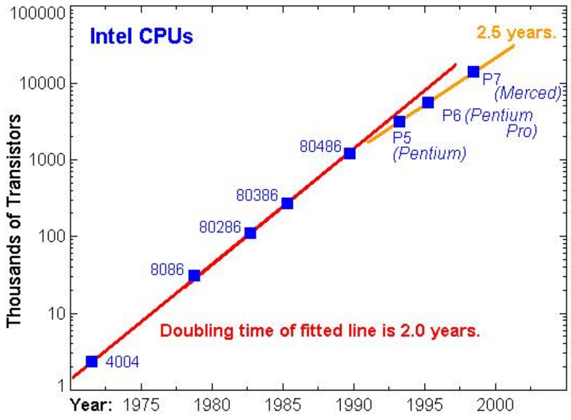
Quantum Computing is the area of study focused on developing computing methods based on the principle of quantum theory. Quantum Physics explains the nature and behaviour of energy and matter on the quantum (atomic and subatomic) scale. Elementary particles such as protons, neutrons and electrons can exist in two or more states at a time. This fundamental behaviour is utilized in designing the quantum computation processing units. Quantum computing uses a combination of bits of 1’s, 0’s and both 1 and 0 at a time to perform computational tasks with greater efficiency.

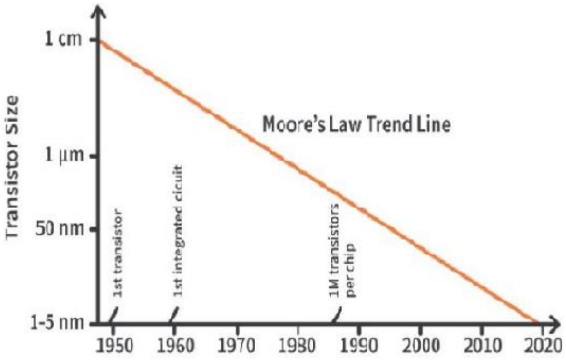
In Quantum computing, the information is encoded in quantum system such as atoms, ions or quantum dots.

Moore’s law & its end

In 1965, Gordon E. Moore—co-founder of Intel—postulated that “the number of transistors in a IC chip doubles about every eighteen months”. This is also known as Moore's Law.

Moore made this statement based on noticing emerging trends in chip manufacturing industry and his prediction became the golden rule known as Moore's Law. Moore predicted that it would continue to improve at an exponential rate for every 2 years. Semiconductor industry has followed his prediction to guide long term planning and to set targets for R&D since then functioning to some extent. Here is a graphical representation.





According to Moore’s law, the number of transistors per integrated circuit chip is doubles approximately every 18 – 24 months. The present limit is approximately 10^8 transistors per chip and the typical size of circuit components is of the order of 100 nanometers. That means, we have reached the atomic size for storing a single bit of information and quantum effects have become unavoidably dominant. Taking all these factors into consideration, it is necessary to look for alternative ways of computing methods. 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 problems of classical computing.

Differences between classical and quantum computing

Key points	classical computing	quantum computing
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	Circuits implemented in microscopic technologies.
Data processing	Data processing is carried out by logic and in sequential order.	Data processing is carried out by quantum logic at parallel instances.

Concept of bit and qubit and its properties of quibits:

Bit: A digital computer stores and processes information using bits which can be either 0 or 1. Physically, a bit can be anything that has two distinct configurations: one represented by "0", and the other represented by "1". It could be a system with two distinct and distinguishable possibilities. In modern computing and communications, bits are represented by the absence or presence of an electrical signal, encoding "0" and "1" respectively.

Qubit is the physical carrier of quantum information. It is the quantum version of a bit, and its quantum state can be written in terms of two levels, labelled $|0\rangle$ and $|1\rangle$.

$|\ \rangle$ this notation is known as 'ket' notation and $\langle\ |$ is known as 'brac' notation. Both are together called as Dirac notations 'Ket' are analogous to a column vector. They are also called basis vectors and represented by two-dimensional column vectors as follows

$$|\mathbf{0}\rangle = \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix} \text{ and } \quad |\mathbf{1}\rangle = \begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix}$$

The qubit can be in any one of the two states as well as in the superposed state simultaneously. In quantum computation two distinguishable states of a system are needed to represent a bit of data.

For example, two states of an electron orbiting a single atom. Spin up is taken as $|1\rangle$ and spin down is taken as $|0\rangle$. Similarly ground state energy level is $|0\rangle$ and excited state level is $|1\rangle$

Superposition of two states:

The difference between qubits and classical bits is that a qubit can be in a linear combination (superposition) of the two states $|0\rangle$ and $|1\rangle$.

For ex, if $\propto$ and β are the probability amplitudes of electron in ground state (ie, in $|0\rangle$ state) and in excited state (ie, in $|1\rangle$ state) then the linear combination of two states is

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

The numbers α and β are complex but due to normalization conditions

$$|\propto|^2 + |\beta|^2 = 1.$$

Here $|\propto|^2$ is the probability of finding $|\psi\rangle$ in state $|0\rangle$ and

$|\beta|^2$ is the probability of finding $|\psi\rangle$ in state $|1\rangle$.

So, that when a qubit is measured, it only gives either '0' or '1' as the measurement result – probabilistically.

Consider the following example of qubit representation

$$|\Psi\rangle = \left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\right)|0\rangle + \left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\right)|1\rangle$$

$$\therefore \propto = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\ and\ \ \beta = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}$$

$$|\propto|^2 = |\beta|^2 = 1/2$$

This means that with 50% probability the qubit will be found in $|0\rangle$ state as well as in $|1\rangle$ state. The superposed states are also called as space states where as $|0\rangle$ and $|1\rangle$ are called basis states.

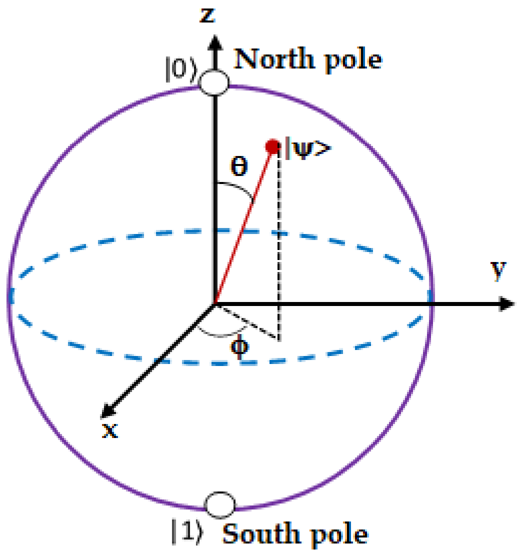
Properties of qubits

1. Qubits make use of discrete energy state particles such as electrons and photons.
2. Qubits exists in two quantum state $|0\rangle$ and $|1\rangle$ or in a linear combination of both states. This is known as superposition.
3. Unlike classical bits, qubit can work with the overlap of both 0 & 1 states.

   For ex, a 4-bit register can store one number from 0 to 15 (because of $2^n = 2^4=16$), but 4-qubit register can store all 16 numbers.
4. When the qubit is measured, it collapses to one of the two basis states $|0\rangle$ or $|1\rangle$
5. Quantum entanglement and quantum tunnelling are two exclusive properties of qubit.
6. **6.** State of the qubits is represented using Bloch sphere.

Representation of Qubits by Bloch Sphere: (single qubit state)

Bloch sphere is an imaginary sphere which is used to represent pure single-qubit states as a point on its surface. It has unit radius. Its North Pole and South Pole are selected to represent the basis states namely $|0\rangle$ and $|1\rangle$. North Pole represents $|0\rangle$ (say spin up↑) and South Pole represents $|1\rangle$ (say spin down ↓). All other points on the sphere represent superposed states (ie, state space). Bloch sphere allows the state of a qubit to be represented in spherical coordinates (ie, r, θ and ϕ). It is as follows



The state qubit |ψ⟩ on the Bloch sphere makes an angle θ with z-axis and its projection (azimuth) makes angle ϕ with x-axis as shown. It is clear from the fig that $0 < \theta < \pi$ and $0 < \phi < 2\pi$.

|ψ⟩ is represented as

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

It can be proved that

$$|\Psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle \quad ---(1)$$

Using this equation we can represent |ψ⟩ for different θ and ϕ as follows

Case-1: let θ = 0 and ϕ = 0, then eq (1) becomes

$$|\Psi\rangle = \cos 0|0\rangle + e^{i0}\sin 0|1\rangle = |0\rangle + 0$$

$$\therefore |\Psi\rangle = |0\rangle$$

Case-2: let θ = π and ϕ = 0, then eq (1) becomes

$$|\Psi\rangle = \cos(\pi/2)|0\rangle + e^{i0}\sin(\pi/2)|1\rangle = 0 + |1\rangle$$

$$\therefore |\Psi\rangle = |1\rangle$$

Case-3: let θ = π/2 and ϕ = 0, then eq (1) becomes

$$|\Psi\rangle = \cos(\pi/4)|0\rangle + e^{i0}\sin(\pi/4)|1\rangle$$

$$|\Psi\rangle = \left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\right)|0\rangle + \left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\right)|1\rangle$$

$$|\Psi\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

Case-4: let θ = π/2 and ϕ = π, then eq (1) becomes

$$|\Psi\rangle = \cos(\pi/4)\,|0\rangle + e^{i\pi}\sin(\pi/4)\,|1\rangle$$

$$|\Psi\rangle = \left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\right)|0\rangle - \left(\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\right)|1\rangle$$

$$|\Psi\rangle = \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

In the above discussion we have represented only single qubit state. Bloch sphere is a nice visualization of single qubit states.

Representation of Multiple Qubits (Two qubits and Extension to N qubits):

Two qubits:

Consider two qubits. They can be in any one of four possible states represented as |00⟩, |01⟩, |10⟩ and |11⟩.

$$|00\rangle=\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \quad |01\rangle=\begin{bmatrix}0\\1\\0\\0\end{bmatrix} \quad |10\rangle=\begin{bmatrix}0\\0\\1\\0\end{bmatrix} \quad |11\rangle=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

The state qubit is (ie, linear combination of these four)

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

For 2 qubit system we have 4 complex amplitudes namely α_{00}, α_{01}, α_{10} and α_{11}. According to normalization condition

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Similarly if there are 3 qubits there will be 8 complex amplitudes.

In general for N qubits, there will be having 2^N complex amplitudes. This means that a basis state is represented by a number 0 to 2^{N-1}.

The superposition state is represented as

$$|\Psi\rangle = \sum_{x=0}^{2^{N-1}} \alpha_x |\mathrm{x}\rangle$$

Qubit has two quantum states similar to the classical binary states. The qubit can be in any one of the two states as well as in the superposed state simultaneously.

Dirac representation and Matrix operations:

In Quantum mechanics, Bra-Ket notation is a standard notation for describing quantum states. The notation | ⟩ is known as 'ket' notation and ⟨ | is known as 'bra' notation. Both are together called as Dirac notations.

Matrix representation of 0 and 1 states:

Consider a quantum state ψ in a vector space represented by $|\psi\rangle$. The notation $|\rangle$ indicates that the object is a vector and is called a ket vector. The examples of such ket vectors are like $|\psi\rangle$, $|\phi\rangle$ and $|u\rangle$ etc.

The wave function could be expressed in ket notation as $|\psi\rangle$ (ket Vector), ψ is the wave function.

Hence, any arbitrary state can be represented as

$$|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix} \quad \text{or} \quad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

The 'ket' vector typically represented as a column vector and 'bra' vector typically represented as a row vector. The matrix for of the states $|0\rangle$ and $|1\rangle$ as follows;

$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$ ket notations

$\langle 0| = [1\ 0]$ $\langle 1| = [0\ 1]$ − − − − − bra notations

Operators and matrices:

An operator is a mathematical rule that transform a given function into another function. Consider an operator 'A' transforms the vector $|\mathrm{a}\rangle$ to another vector $|b\rangle$, it can be written as

$$\widehat{\mathrm{A}}|\mathrm{a}\rangle \ = |\mathrm{b}\rangle$$

There are different types of operators like Linear operator, Identity operator, Null operator, Inverse operator, Singular & non-singular operator etc.

Identity operator I :

The identity operator is an operator which, operating on a function, leaves the function unchanged i.e. $I\ |a\rangle$ = $|a\rangle$ It is given in matrix form by

$$\mathrm{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

This is also called as identity matrix. There will be no change when I operate on either $|0\rangle$ state or $|1\rangle$ state. It is explained as follows

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

$$\therefore \mathrm{I}|0\rangle = |0\rangle$$

Similarly

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

$$\therefore \mathrm{I}|1\rangle = |1\rangle$$

Identity matrix acts as number 1. It is always a square matrix.

Conjugate matrices:

If the elements in a matrix A are complex numbers, then the matrix obtained by the corresponding conjugate complex elements is called the conjugate of A and is denoted by $A*$.

For example

if $\mathrm{A} = \begin{bmatrix} 0 & \mathrm{i} \\ -\mathrm{i} & 0 \end{bmatrix}$ then $\mathrm{A}^* = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}$

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

Transpose matrices

If columns and rows of a matrix A are interchanged then the resultant matrix is transpose of A and represented as A^T .

For example ,

if $A = \begin{bmatrix} 0 & 1 \\ -i & 0 \end{bmatrix}$ then $A^{*} = \begin{bmatrix} 0 & -i \\ 1 & 0 \end{bmatrix}$

if $A = \begin{bmatrix} 1 & 2i \\ 4i+1 & 0 \end{bmatrix}$ then $A^{*} = \begin{bmatrix} 1 & 4i+1 \\ 2i & 0 \end{bmatrix}$

Hermitian matrices:

The transpose of complex conjugate of a matrix is known as Hermitian operator and the resultant matrix is known as Hermitian matrix. It is represented by $A^{\dagger}$

Let A be a matrix, A* be its complex conjugate and A^{*T} is its transpose then its Hermitian matrix is $A^{\dagger} = A^{*T}$

if $A = \begin{bmatrix} 1 & 2i \\ 4i+1 & 0 \end{bmatrix}$ $A^{*} = \begin{bmatrix} 1 & -2i \\ -4i+1 & 0 \end{bmatrix}$ then $A^{\dagger} = \begin{bmatrix} 1 & -4i+1 \\ -2i & 0 \end{bmatrix}$

Unitary matrices:

Matrix A is said to be unitary if it produces an identity matrix I when multiplied by its conjugate transpose $AA^{\dagger} = I$

In other words, A is a unitary matrix if its conjugate transpose is equal to its reciprocal, ie

$$A^{\dagger} = \frac{I}{A} = \frac{1}{A} = A^{-1}$$

we can show that $A = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$

Column and Row Matrices and their inner product:

The Column Vectors are called ket Vectors denoted by $|\psi\rangle$ and are represented by Column Matrices.

The Row Vectors are called Bra Vectors denoted by $\langle\phi|$ and are represented by Row Matrices.

Let us consider a ket vector represented in the form of a column matrix.

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

The Row Matrix is represented as

$$\langle\psi| = [\alpha_1^{*} \quad \beta_1^{*}]$$

Here, $\begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}^{\dagger} = [\alpha_1^{*} \quad \beta_1^{*}]$

Thus the Bra is the complex conjugate of ket and vice versa.

Inner product: The inner product of two vectors U and V in the complex space is a function that takes U and V as inputs and produces a complex number as output.

In terms of Dirac notation, the inner product is given as $\langle U|V\rangle$ = C

In matrix form U and V are written a

$$|\mathbf{U}\rangle = \begin{bmatrix}\mathbf{x_1}\\ \mathbf{y_1}\end{bmatrix} \text{and} \quad |\mathbf{V}\rangle = \begin{bmatrix}\mathbf{x_2}\\ \mathbf{y_2}\end{bmatrix}$$

Their inner product is written as $\langle U|V\rangle$, but $\langle U|$ is equal to conjugate transpose of $|U\rangle$

$ie,$ $\langle U|$ = $|U^*\rangle^{-1}$ = $|U\rangle^{\dagger}$ = $[x_1{}^* \; y_1{}^*]$

$\therefore \langle U|V\rangle = [x_1{}^* \; y_1{}^*]\begin{bmatrix}\mathrm{x}_2\\ \mathrm{y}_2\end{bmatrix} = x_1{}^*x_2 + y_1{}^*y_2$

The square root of the inner product of a vector with itself is also called as norm or the length of the vector. It is given by $|\mathrm{U}| = \sqrt{\langle \mathrm{U}|\mathrm{U}\rangle}$

Ex: Find the inner product of

$$|\mathbf{U}\rangle = \begin{bmatrix}\mathbf{3+i}\\ \mathbf{4-i}\end{bmatrix} \text{and} \quad |\mathbf{V}\rangle = \begin{bmatrix}\mathbf{3i}\\ \mathbf{4}\end{bmatrix}$$

First we shall find the conjugate transpose of $|U\rangle$

$$|\mathrm{U}^*\rangle = \begin{bmatrix}3-\mathrm{i}\\ 4+\mathrm{i}\end{bmatrix}$$

$$|\mathrm{U}\rangle^{\dagger} = [3-\mathrm{i} \quad 4+\mathrm{i}]$$

$$\therefore \langle U| = |\mathrm{U}\rangle^{\dagger} = [3-\mathrm{i} \quad 4+\mathrm{i}]$$

$$\langle \mathrm{U}|\mathrm{V}\rangle = [3-\mathrm{i} \quad 4+\mathrm{i}]\begin{bmatrix}3\mathrm{i}\\ 4\end{bmatrix}$$

$$\langle \mathrm{U}|\mathrm{V}\rangle = (3-\mathrm{i}) * 3\mathrm{i} +* (4+\mathrm{i})4$$

$$\langle \mathrm{U}|\mathrm{V}\rangle = 9\mathrm{i} + 3 + 16 + 4i$$

$$\langle \mathrm{U}|\mathrm{V}\rangle = 13\mathrm{i} + 19$$

Orthogonality:

If the inner product of two vectors is equal to 0 then they are said to be orthogonal (or perpendicular) to each other.

If $\langle U|V\rangle$ = 0 then $|U\rangle$ and $|V\rangle$ are perpendicular.

Consider,

$$|\mathbf{0}\rangle = \begin{bmatrix}\mathbf{1}\\ \mathbf{0}\end{bmatrix} \quad \text{and} \quad |\mathbf{1}\rangle = \begin{bmatrix}\mathbf{0}\\ \mathbf{1}\end{bmatrix}$$

$$\langle 0|1\rangle = [\mathbf{1} \quad \mathbf{0}]\begin{bmatrix}\mathbf{0}\\ \mathbf{1}\end{bmatrix} = 0$$

Hence $|0\rangle$ is perpendicular to $|1\rangle$

The most important property of the inner product of a vector with itself is equal to one ie, $\langle\psi|\psi\rangle = 1$

This is known as normalization condition. The physical significance of normalization is that the "probability amplitude" of the quantum system

Orthonormality: If each element of a set of vectors is normalized and the elements are orthogonal with respect to each other, we say the set is orthonormal.

Consider the set $|\mathbf{0}\rangle = \begin{bmatrix}\mathbf{1}\\\mathbf{0}\end{bmatrix}$ and $|\mathbf{1}\rangle = \begin{bmatrix}\mathbf{0}\\\mathbf{1}\end{bmatrix}$

$\langle 0|0\rangle = [\mathbf{1} \quad \mathbf{0}]\begin{bmatrix}\mathbf{1}\\\mathbf{0}\end{bmatrix} = 1$ normalized

$\langle 0|1\rangle = [\mathbf{1} \quad \mathbf{0}]\begin{bmatrix}\mathbf{0}\\\mathbf{1}\end{bmatrix} = 0$ orthogonal

$\langle 1|1\rangle = [\mathbf{0} \quad \mathbf{1}]\begin{bmatrix}\mathbf{0}\\\mathbf{1}\end{bmatrix} = 1$ normalized

$\langle 1|0\rangle = [\mathbf{0} \quad \mathbf{1}]\begin{bmatrix}\mathbf{1}\\\mathbf{0}\end{bmatrix} = 0$ orthogonal

Hence set of $|0\rangle$ and $|1\rangle$ is orthonormal.

From the above relations, if states $|\psi\rangle$ and $|\phi\rangle$ are said to be orthonormal if

1. $|\psi\rangle$ and $|\phi\rangle$ are normalized.
2. $|\psi\rangle$ and $|\phi\rangle$ are orthogonal to each other.

Probability

Let us consider a Quantum State

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

$$|\psi\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

The inner product $\langle\psi|\psi\rangle$ is given by

$$\langle\psi|\psi\rangle = [\alpha^* \quad \beta^*]\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \alpha^*\alpha + \beta^*\beta$$

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

This could also be written as $|\psi|^2 = \psi\ \psi^*$

Thus the above equation represents Probability Density. As per the principle of Normalization

$$|\psi|^2 = \psi\ \psi^* = \langle\psi|\psi\rangle = 1 = |\alpha|^2 + |\beta|^2$$

Thus it implies $|\psi\rangle$ is normalized.

Pauli Matrices:

These are the 2 × 2 complex matrices introduced by Pauli in order to account for the interaction of the spin with an external electromagnetic field. They are given by

$$\sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Properties of Pauli matrices:

- Square Pauli matrices gives identity matrix I

$$X^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Similarly,

$$Y^2 = I \quad \text{and} \quad Z^2 = I$$

- Pauli matrices are unitary matrix.

$$XX\dagger = 1,\ YY\dagger = 1 \quad \text{and}\ ZZ\dagger = 1$$

- Pauli matrices are Hermitian:

Let A be a matrix, A* be its complex conjugate and $A\dagger$ is its transpose. If A = $A\dagger$ then the matrix is Hermitian.

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

$$Y^* = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$

$$Y^\dagger = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Y = Y^\dagger$$

Operation of Pauli Matrices on 0 and 1 states

Three Pauli matrices X, Y and Z operates on states |0⟩ and |1⟩ as follows

- **X operating on |0⟩ and |1⟩**

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

$$X|0\rangle = |1\rangle$$

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

$$X|1\rangle = |0\rangle$$

Since X inverts each input (ie, |0⟩ becomes |1⟩ and |1⟩ becomes|0⟩).

It is also called as bit-flip gate.

If a superposed qubit goes through X gate, the result will be

$$X|\psi\rangle = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\beta\\\alpha\end{bmatrix} = \alpha|1\rangle + \beta|0\rangle$$

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

- **Y operating on |0⟩ and |1⟩**

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

$$Y|0\rangle = i|1\rangle$$

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

$$Y|1\rangle = -i|0\rangle$$

If a superposed qubit goes through Y gate, the result will be

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

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

- **Z operating on |0⟩ and |1⟩**

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

$$Z|0\rangle = |0\rangle$$

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

$$Z|1\rangle = -|1\rangle$$

If a superposed qubit goes through Y gate, the result will be

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

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

Quantum Gates:

A quantum gate is a very simple computing device that performs quantum operation on qubits. Quantum gates are one of the essential parts of a quantum computer and are the building blocks of all quantum algorithms.

Quantum gates are mathematically represented as transformation matrices which operate on inputs to give outputs.

There are different types of quantum gates. Single-qubit gates and multiple qubit gates. These gates can flip a qubit from 0 to 1 as well as allowing superposition states to be created.

Single-Qubit Gates:

Single qubit inputs are $|0\rangle$ to $|1\rangle$ and can be represented by matrix forms as

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

Single Qubit Gates are X- gate, Y-gate, Z- gate, H –gate, S-gate, T-gate.

1. X – Gate or Quantum Not Gate

X-gate is the single qubit input gate and is also called as Pauli X – gate or quantum NOT gate.

The Matrix form of X is given by

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

Action of the X-gate on inputs: When X gate operates of inputs $|0\rangle$, $|1\rangle$, $|\psi\rangle$;

When X operates on $|0\rangle$ and $|1\rangle$ the output will be inverted (ie,$|0\rangle$ becomes $|1\rangle$ and $|1\rangle$ becomes$|0\rangle$)

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

$$\mathrm{X}|0\rangle = |1\rangle$$

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

$$\mathrm{X}|1\rangle = |0\rangle$$

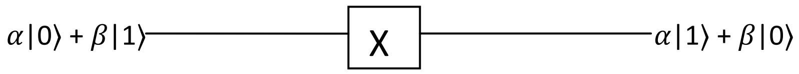
Since X inverts each input it is also called as bit-flip gate.

If a superposed qubit goes through X gate, the result will be

$$\mathrm{X}|\psi\rangle = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}\alpha\\\beta\end{bmatrix} = \begin{bmatrix}\beta\\\alpha\end{bmatrix} = \alpha|1\rangle + \beta|0\rangle$$

$$\mathrm{X}|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

Gate representation is


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

Truth table is

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

2. **Y – Gate** : Y-gate is the single qubit input gate. This is also called as Pauli Y – gate.

The matrix form of Y gate is $\mathrm{Y} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}$

Action of Y gate on inputs : When Y operates on $|0\rangle$ and $|1\rangle$

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

$$\mathrm{Y}|0\rangle = \mathrm{i}|1\rangle$$

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

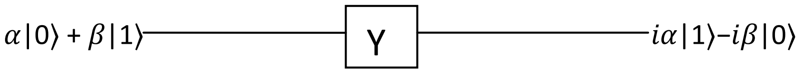
$$\mathrm{Y}|1\rangle = -\mathrm{i}|0\rangle$$

If a superposed qubit goes through Y gate, the result will be

$$\mathrm{Y}|\psi\rangle = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} -\mathrm{i}\beta \\ \mathrm{i}\alpha \end{bmatrix} = -\mathrm{i}\beta|0\rangle + \mathrm{i}\alpha|1\rangle$$

$$\mathrm{Y}|\psi\rangle = -\mathrm{i}\beta|0\rangle + \mathrm{i}\alpha|1\rangle$$

Gate representation is



Truth table is

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

3. **Z – Gate** : Z-gate is the single qubit input gate. This is also called as Pauli Z – gate.

The matrix form of Z gate is

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

Action of Z gate on inputs: When Z operates on $|0\rangle$ and $|1\rangle$ the phase will change. Hence this is also called as phase-flip gate

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

$$Z|0\rangle = |0\rangle$$

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

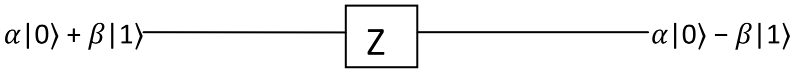
$$Z|1\rangle = -|1\rangle$$

If a superposed qubit goes through Y gate, the result will be

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

$$Z|\psi\rangle = \alpha|0\rangle - \beta|1\rangle$$

Gate representation is

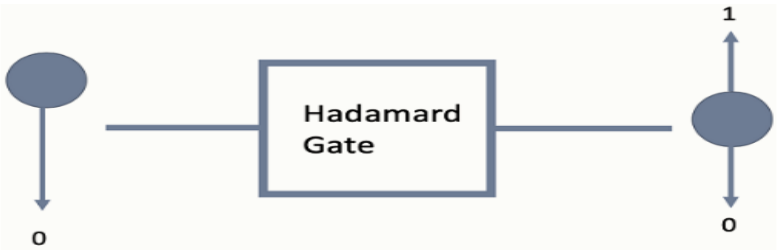

$\alpha|0\rangle + \beta|1\rangle$
Z
$\alpha|0\rangle - \beta|1\rangle$

The truth tables for X, Y and Z gates are as follows;

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

4. **Hadamard Gate (H-gate)** – It is a single qubit gate and is also gate to superposition. H gate acts on single qubit input and produce superposition state output. Matrix form of H gate and its symbol is

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



Action of H gate on inputs:

Let us find out what happens when Hadamard gate operates on a qubit that is in the |0⟩ state

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\mathrm{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Let us find out what happens when Hadamard gate operates on a qubit that is in the |1⟩ state.

$$\mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

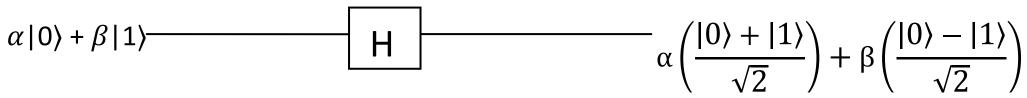
$$\mathrm{H}|0\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

If a superposed qubit goes through H gate, the result will be

$$\mathrm{H}|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\alpha + \beta\\ \alpha - \beta\end{bmatrix} = \left(\frac{\alpha + \beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha - \beta}{\sqrt{2}}\right)|1\rangle$$

$$\mathrm{H}|\psi\rangle = \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Gate representation is


$\alpha|0\rangle + \beta|1\rangle$
H
$\alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

The truth table is as follows

Input	**Output**
$|0\rangle$	$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$|1\rangle$	$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$\alpha|0\rangle + \beta|1\rangle$	$\alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

Note: Difference between X, Y, Z and H gates is that in X, Y and Z gates, output is in single state whereas in H gate output is superposed state.

5. Phase Gate (S Gate):

It is a single qubit gate. The Phase gate or S gate is a gate that transfers $|0\rangle$ into $|0\rangle$ and $|1\rangle$ into $i|1\rangle$. The matrix form of S gate is

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

Action of S gate on inputs:

Consider S gate apply to a state $|0\rangle$ it will remain same

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

$$\mathrm{S}|0\rangle = |0\rangle$$

If S gate apply to a state $|1\rangle$ it will be transformed into $i|1\rangle$

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

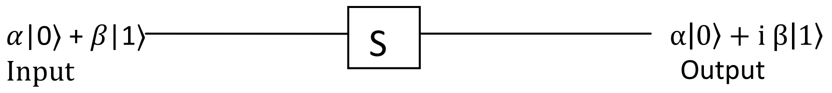
$$\mathrm{S}|1\rangle = \mathrm{i}|1\rangle$$

S gate apply to the state $\alpha|0\rangle + \beta|1\rangle$ it transforms to the state $\alpha|0\rangle + i\beta|1\rangle$

$$\mathrm{S}|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \mathrm{i}\beta \end{bmatrix}$$

$$\mathrm{S}|\psi\rangle = \alpha|0\rangle + \mathrm{i}\,\beta|1\rangle$$

The S gate representation is as follows



The truth table is as follows

Input	**Output**
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\mathrm{i}\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + \mathrm{i}\,\beta\|1\rangle$

6. T- Gate : It is a single qubit gate and it is also called π/8 gate.

Its matrix form is

$$\mathrm{T} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\pi/4} \end{bmatrix}$$

Action of T gate on inputs:

If T gate operates on input is $|0\rangle$ then the output is also $|0\rangle$

$$T|0\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

$$T|0\rangle = |0\rangle$$

If T gate operates on input is $|1\rangle$ then the output is also $e^{i\pi/4}|1\rangle$

$$T|0\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = e^{i\pi/4}\begin{bmatrix}0\\1\end{bmatrix} = e^{i\pi/4}|1\rangle$$

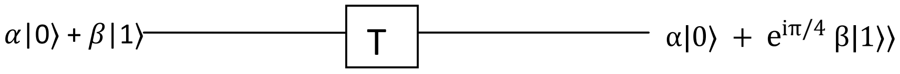
$$T|0\rangle = e^{i\pi/4}|1\rangle$$

If T gate operates on superposed state $\alpha|0\rangle + \beta|1\rangle$, It transforms to $\alpha|0\rangle + e^{i\pi/4}$ $\beta|1\rangle$

$$T|\psi\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{\frac{i\pi}{4}}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\alpha\\ \beta e^{\frac{i\pi}{4}}\end{bmatrix} = \alpha|0\rangle + e^{i\pi/4}\,\beta|1\rangle$$

$$T|\psi\rangle = \alpha|0\rangle + e^{i\pi/4}\,\beta|1\rangle$$

T Gate representation is


$\alpha|0\rangle + \beta|1\rangle$
T
$\alpha|0\rangle + e^{i\pi/4}\,\beta|1\rangle\rangle$

The truth table is as follows

Input	**Output**
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$e^{i\pi/4}\|1\rangle$
$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|0\rangle + e^{i\pi/4}\,\beta\|1\rangle$

Multiple Qubit gates: Quantum gates operating on multiple qubits are called as multiple qubit gates. Multiple Qubit Gates operate on Two or More input Qubits. Multiple qubit consists of control gate and target gate. The action of gate as follows;

i) The Target qubit is altered only when the control qubit is $|1\rangle$, and

ii) The control qubit remains unaltered during the transformations.

For two qubits, inputs qubits are $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$

For three qubits, inputs qubits are $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$ and $|111\rangle$

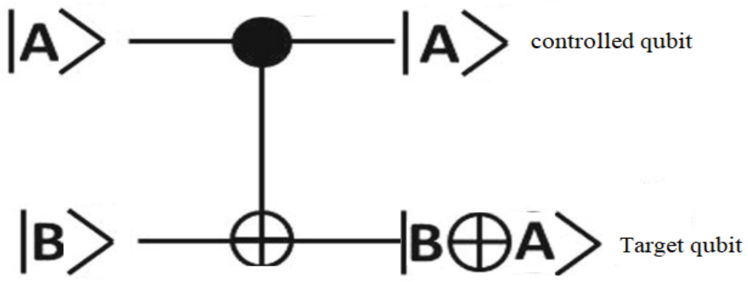
In multiple qubit gate, the input qubit applied in the form like $|AB\rangle$, first term $|A\rangle$ goes to control qubit and the second term $|B\rangle$ goes to target qubit.

Some of the multiple qubit gate are as follows; Controlled gate (CNOT gate), Swap gate, Controlled Z gate and Toffoli gate (CCNOT gate)

1. Controlled Gate (CNOT)

The CNOT gate is a two-qubit operation, where the first qubit is referred as the control qubit $|A\rangle$ and the second qubit as the target qubit $|B\rangle$. If the control qubit is $|1\rangle$ then it will flip the target qubit state from $|0\rangle$ to $|1\rangle$ or from $|1\rangle$ to $|0\rangle$. When the control qubit is in state $|0\rangle$ then the target qubit remains unchanged.

The symbolic representation is as follows. The upper line represents control qubit and bottom line represents target qubit.



NOTE: In diagram the control qubit is represented by ● and target is represented by ⊕

In the combined qubit, first term is control qubit and the second term is target qubit. For ex, in $|AB\rangle$, A is control qubit and B is target qubit

Matrix form of **CNOT** Gate is given by

$$\mathbf{CNOT} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}$$

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

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

i) Operation of CNOT Gate for input $|00\rangle$: $|00\rangle \rightarrow |00\rangle$

Here, control qubit is $|0\rangle$. Hence no change in the state of Target qubit $|0\rangle$.

ii) Operation of CNOT Gate for input |01⟩: |01⟩ → |01⟩

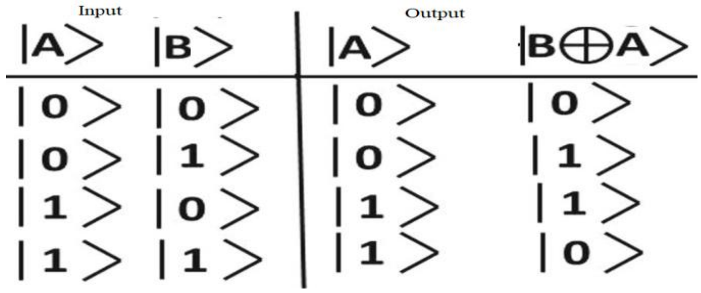
Here, control qubit is |0⟩. Hence no change in the state of Target qubit |1⟩

iii) Operation of CNOT Gate for input |10⟩: |10⟩ → |11⟩

Here, control qubit is |1⟩. Hence the state of Target qubit flips from |0⟩ to |1⟩.

iv) Operation of CNOT Gate for input |11⟩: |11⟩ → |10⟩

Here control qubit is |1⟩. Hence the state of Target qubit flips from |1⟩ to |0⟩.



Input		Output	
|A>	|B>	|A>	|B⊕A>
|0>	|0>	|0>	|0>
|0>	|1>	|0>	|1>
|1>	|0>	|1>	|1>
|1>	|1>	|1>	|0>

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

Input	Output
|00⟩	|00⟩
|01⟩	|01⟩
|10⟩	|11⟩
|11⟩	|10⟩

2. Swap Gate:

SWAP gate is a two qubit operation gate and swaps the state of the two qubits involved in the operation. It contains 3 CNOT gates.

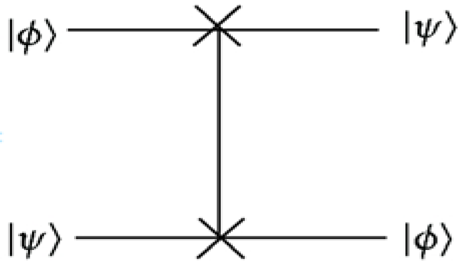
The Matrix representation of the Swap Gate is as follows

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

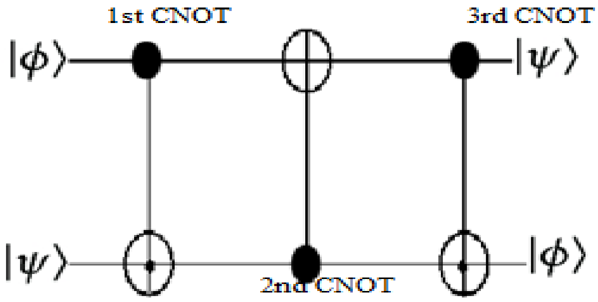
The schematic symbol of swap gate circuit and its equivalent is shown in figure below.

The swap gate is a combined circuit of 3 CNOT gates (1st CNOT gate, 2nd CONT gate and 3rd CNOT gate) and the overall effect is that two input qubits are swapped at the output.

Gate representation is



The Action of the swap gate is as follows.



v) Operation of SWAP Gate for input $|00\rangle$: $|00\rangle \rightarrow |00\rangle$

vi) Operation of SWAP Gate for input $|01\rangle$: $|01\rangle \rightarrow |01\rangle$

vii) Operation of SWAP Gate for input $|10\rangle$: $|10\rangle \rightarrow |11\rangle$

viii) Operation of SWAP Gate for input $|11\rangle$: $|11\rangle \rightarrow |10\rangle$

Gate	**Input to the gate**	**Output of the gate**
1	$|a, b\rangle$	$|a, a \oplus b\rangle$
2	$|a, a \oplus b\rangle$	$|b, a \oplus b\rangle$
3	$|b, a \oplus b\rangle$	$|b, a\rangle$

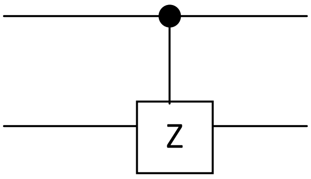
Truth table of the swap gate

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

3. Controlled Z Gate: In Controlled Z Gate, The operation of Z Gate is controlled by a Control Qubit. If the control Qubit is $|A\rangle$ = $|1\rangle$ 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.

$$\textbf{Controlled Z gate} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{-1} \end{bmatrix}$$

The controlled Z gate representation as follows.



Action of controlled Z gate is

ix) Operation of the Gate for input $|00\rangle$: $|00\rangle$ → $|00\rangle$

Control qubit is $|0\rangle$, Z gate remains unchanged.

x) Operation of the Gate for input $|01\rangle$: $|01\rangle$ → $|01\rangle$

Control qubit is $|0\rangle$, Z gate remains unchanged.

xi) Operation of the Gate for input $|10\rangle$: $|10\rangle$ → $|10\rangle$

Control qubit is $|1\rangle$, Z gate remains unchanged.

xii) Operation of the Gate for input $|11\rangle$: $|11\rangle$ → -$|11\rangle$

Control qubit is $|1\rangle$, Z gate flips the state from $|1\rangle$ to -$|1\rangle$.

Truth table of the controlled Z gate

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

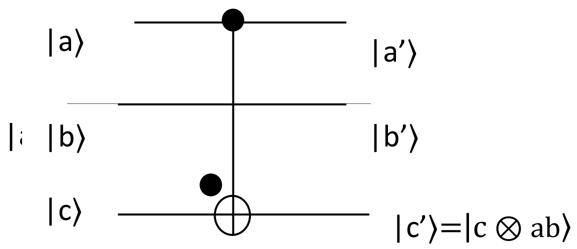
4. Toffoli Gate:

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 the Gate is,.

$$\textbf{Toffoli Gate} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}$$

Gate representation:



Truth Table of Toffoli Gate.

Input to the gate |abc⟩	**Output of the gate** |a'b'c'⟩
|100⟩	|100⟩
|001⟩	|001⟩
|010⟩	|010⟩
|011⟩	|011⟩
|100⟩	|100⟩
|101⟩	|101⟩
|110⟩	|111⟩
|111⟩	|110⟩

Entanglement:

Entangled states are a fundamental concept in quantum computing and quantum mechanics, describing a unique quantum correlation between two or more qubits (quantum bits). In an entangled state, the quantum state of one qubit is inherently linked to the quantum state of another, regardless of the physical distance between them. This connection leads to phenomena that cannot be explained by classical physics.

What are Bell States:

The term Bell pairs actually describes one of four entangled two qubit quantum states, known collectively as the four “Bell states.” Two of the Bell states give an equal superposition such that both of the qubits end up in the same state when measured, with a 50% chance that both will be in either the $|0\rangle|0\rangle$ or $|1\rangle|1\rangle$ state. The other two Bell pairs give an equal superposition such that both of the qubits end in opposite states when measured. This means that if the first qubit is measured in $|0\rangle|0\rangle$, then the second qubit will be measured in $|1\rangle|1\rangle$ and vice versa.

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Applications in Quantum Computing:

1. **Quantum Teleportation**: Entangled states enable the transfer of quantum information (state) from one qubit to another across a distance.
2. **Quantum Cryptography**: Protocols like Quantum Key Distribution (QKD) use entanglement to ensure secure communication.
3. **Quantum Algorithms**: Entanglement is exploited in algorithms like Shor's and Grover's to achieve computational speed-ups.
4. **Error Correction**: Entanglement is essential in quantum error-correcting codes to protect quantum information against decoherence.

5. **Measurement-Based Quantum Computing**: Entangled states form the resource for performing computations in this model of quantum computing.