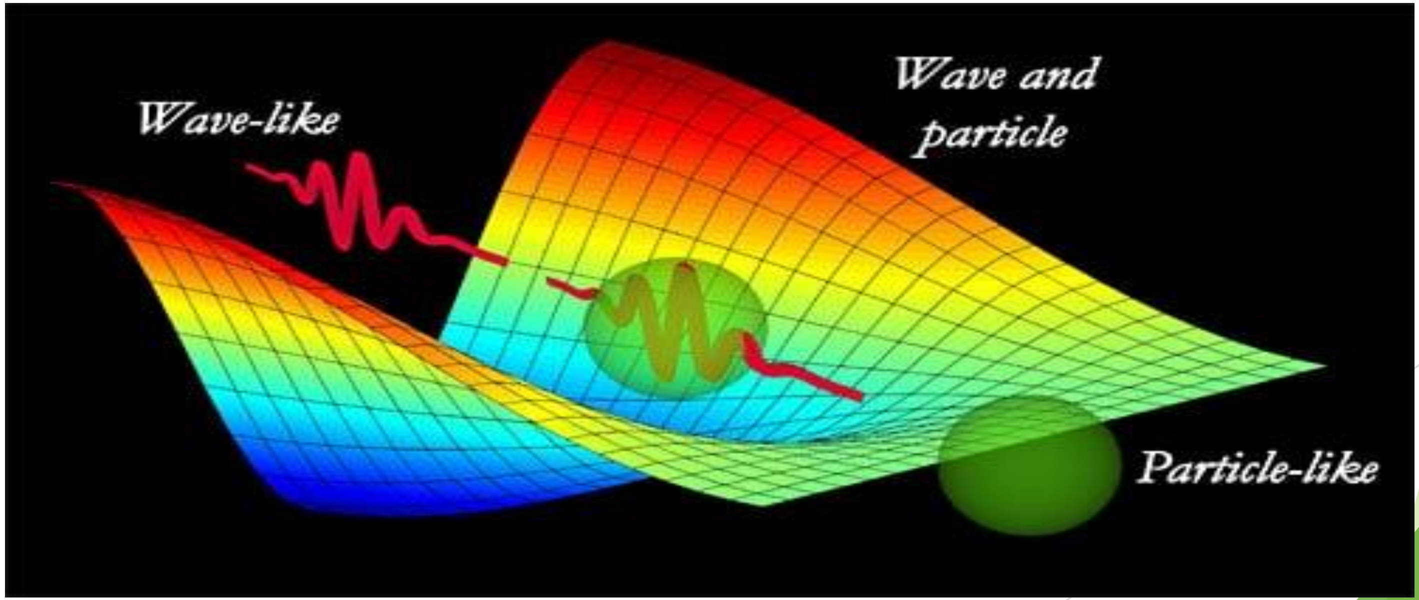
Quantum Object

- Quantum object have both wave’s and particle’s nature.
- Particle exists in a single place at any instant in time.
- We can’t measure the exact position of a wave.
- Everything in universe behaves like both a particle and a wave same time.

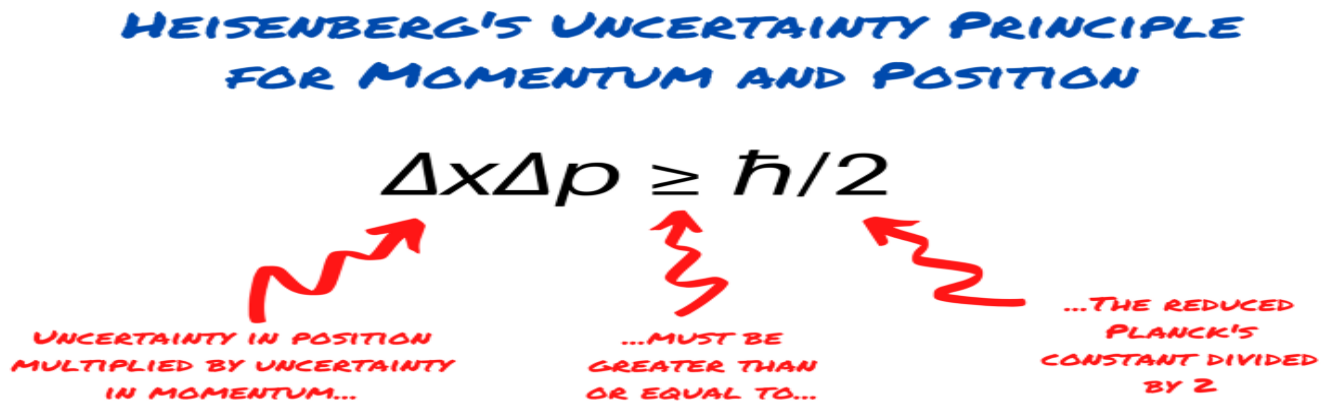


What is a quantum computer?

- A quantum computer is a machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.

Heisenberg Uncertainty Principle

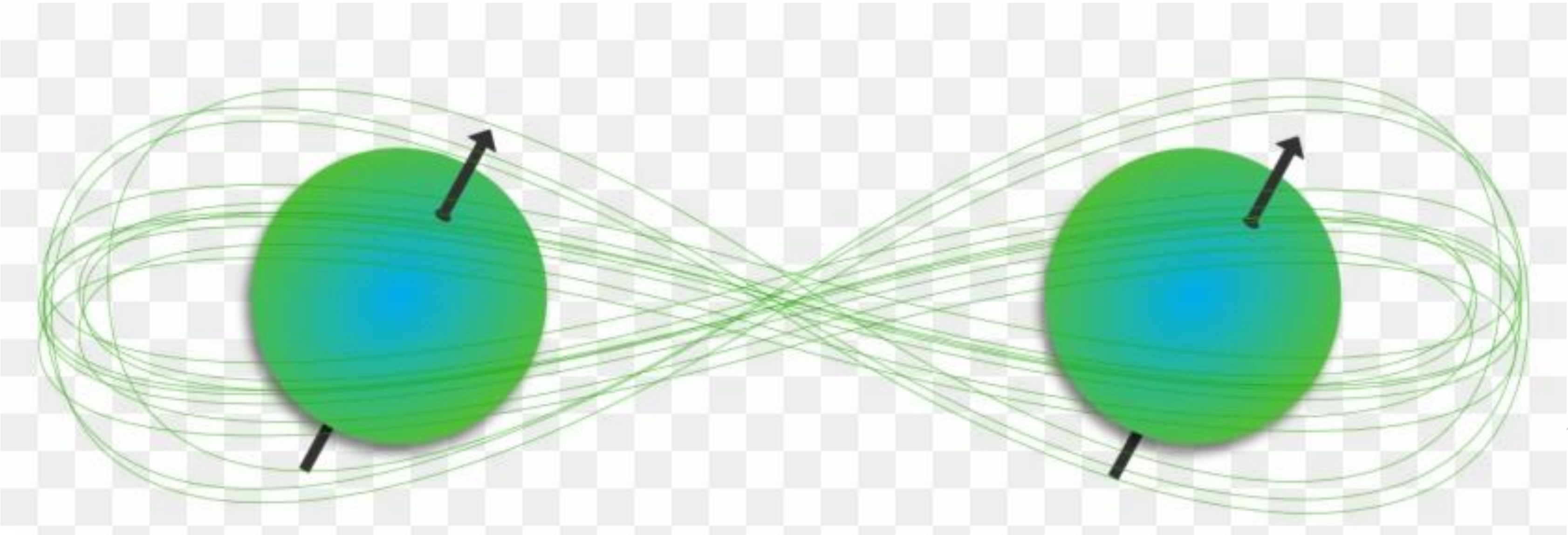
- The uncertainty principle **states that we cannot know both the position and speed of a particle, such as a photon or electron, with perfect accuracy.**
- In other words , you can never simultaneously know the exact position and exact speed of an object.



- Plank's constant is used to describe the behaviour of particles and waves at an atomic scale.

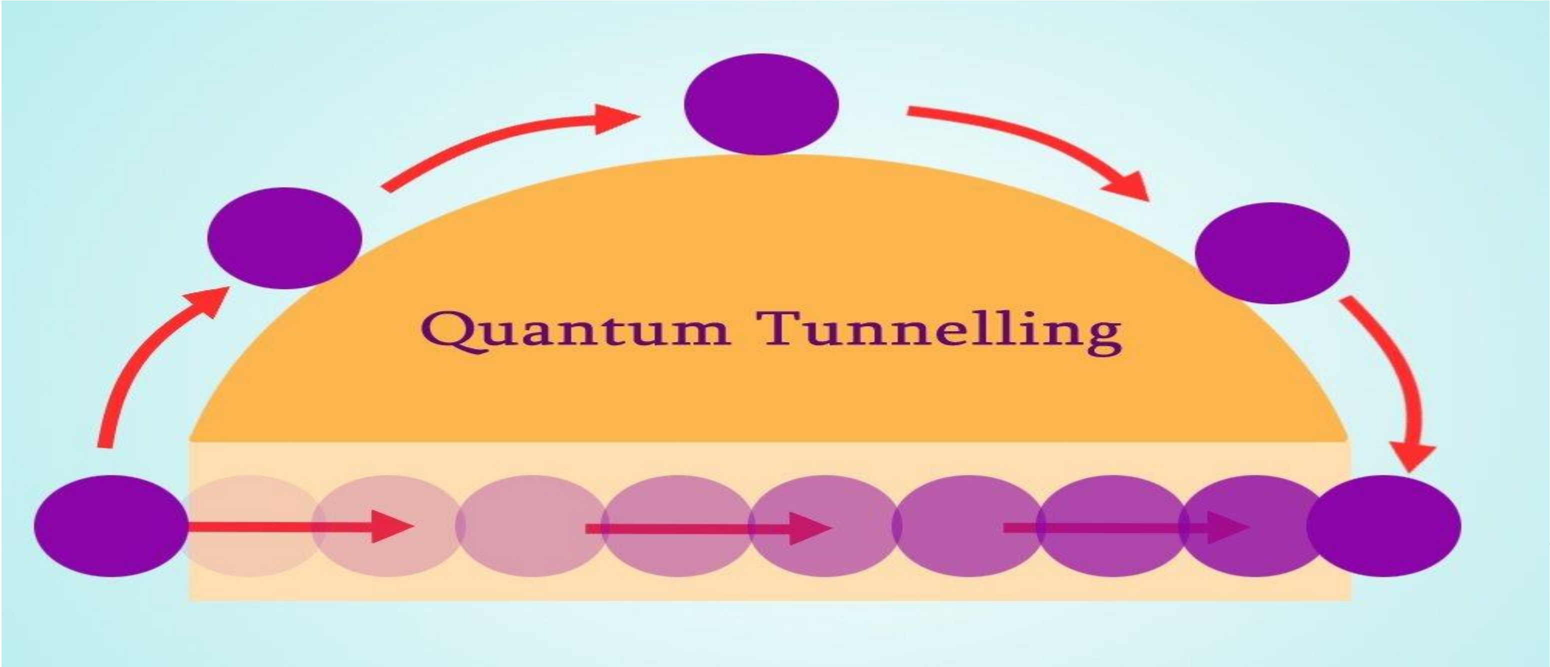
Quantum Entanglement

- Quantum entanglement is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated.
- There is a correlation exist between the spin of the two entangled electrons.



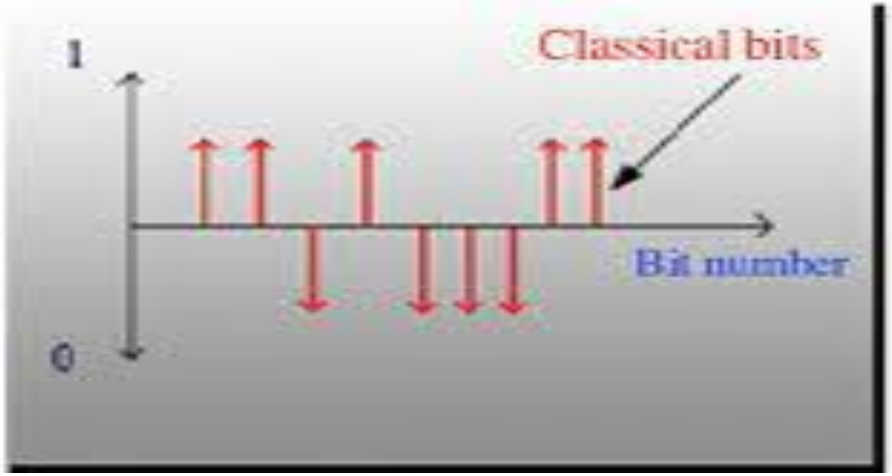
Quantum Tunneling

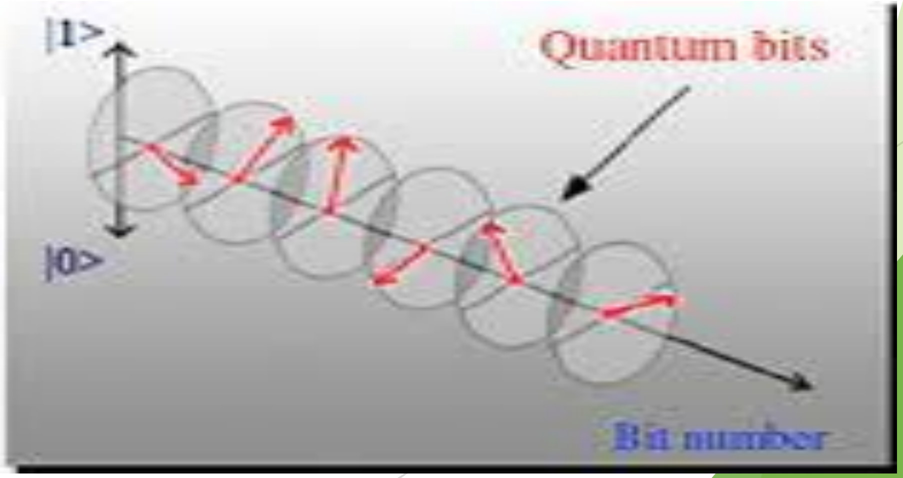
- Tunneling is a quantum mechanical phenomenon when a particle is able to penetrate through a potential energy barrier that is higher in energy than the particle’s kinetic energy.

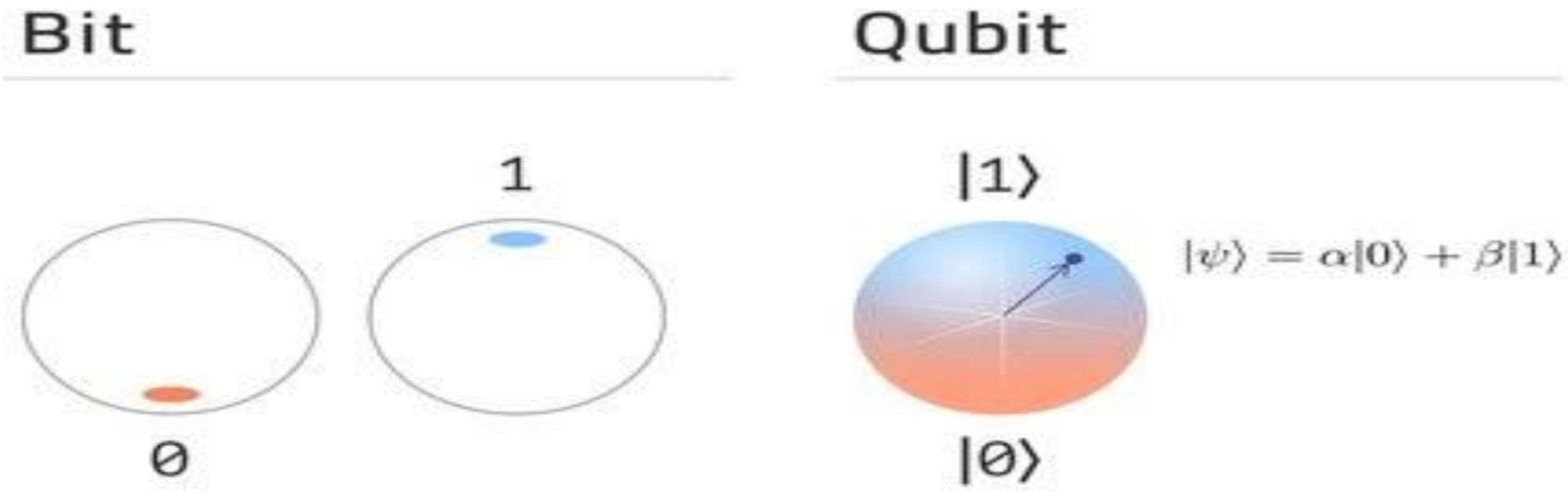


Classical bits v/s Quantum Bits

- In Classical computer , We used 0 and 1 to represent data, they are called classical bits. They can be copied.
- But in case of Quantum computers we used another form to represent data. These are called quantum bits. It cannot be copied.
- A qubit can exist state |0> or state |1> .
- But it can also exist in a superposition of |0> and |1>.
- This is a state that is a linear combination of |0> and |1>







- Here, ∞ and **β** are the amplitude or probability of state 0 and state 1 .
- Modulus squared of α and β gives us the probability of finding the qubit in state |0> and |1>.
- $|\alpha|^2$: Tell us the probability of finding |ψ> in state |0>
- $|\beta|^2$: Tell us the probability of finding |ψ> in state |1>.

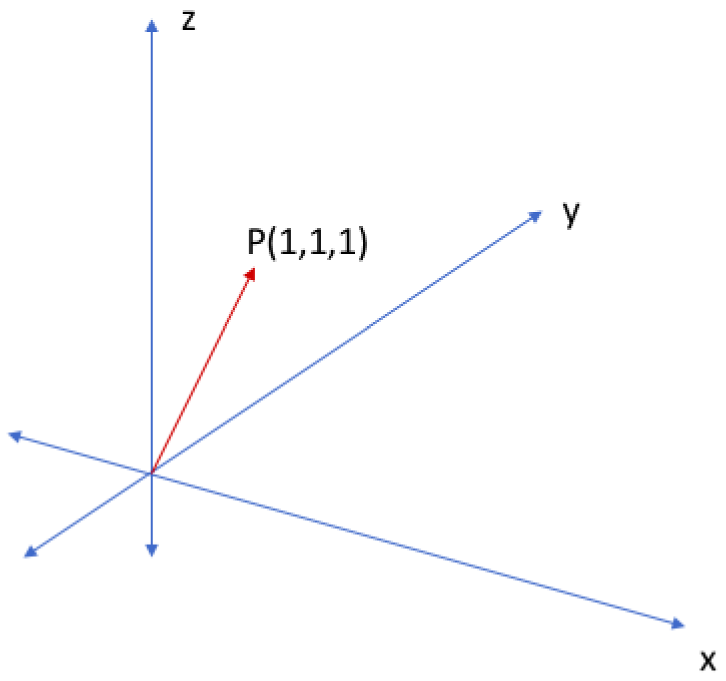
No-Cloning Theorem

- It is impossible to create an independent and identical copy of an arbitrary unknown quantum state.

How to represent a Qubit ?

Vectors

- Vectors are geometrical entities that have magnitude and direction. A vector can be represented by a line with an arrow pointing towards its direction and its length represents the magnitude of the vector.
- $\vec{L} = (Lx, Ly, Lz)$ Here $x, y\ and\ z$ are the components of the vector L. $\vec{L} \in R3$ (set of 3-dimentional vector with three components.)
- We can also represent the vectors as the form $\vec{L} = Lx\hat{\imath} + \text{Ly}\hat{\jmath} + Lz\hat{k}$.
- $i = (1,0,0)$ $j = (0,1,0)$ $k = (0,0,1)$ these are called Basis Vectors

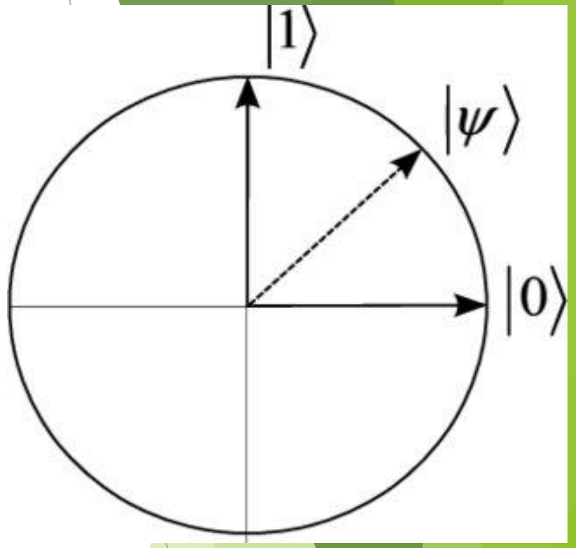


Vector space

- The arena in which quantum computing take place is a mathematical abstraction called a vector space.
- **Linear independent** : If no vector in the set can be expressed as a linear combination(adding two vectors) of other vectors in the set is called linear independent vectors.
- **Basis** : It is a set of linearly independent vectors that can be span full of space.
- **Dimention** : Dimention of a vector space v is equal to the number of elements in the basis set.
- **Span** : The span of vectors ‘v’ and ‘w’ is the set of all their linear combinations.
- Hilbert Space: A unit vector in a k dimensional complex vector space called a Hilbert space

Qubit Representation

- A qubit is represented as a complex vector of size 2.
- State |0> = $\begin{matrix} 1 \\ 0 \end{matrix}$ and State |1>=$\begin{matrix} 0 \\ 1 \end{matrix}$.
- In quantum mechanics “ bra-ket “ or “Dirac” notation is used to denote quantum states.
- This notation uses angle brackets “< “and” >” end a vertical bar “|” to construct “bras and kets”.



Representation of Qubit-Superposition

- Qubit can also present in superposition of states.
- That is in a quantum system,if a particle can be in a state |0> and |1>.Then it can also be in a state $\alpha|0> +\beta|1>$.
- Here α, β are complex numbers.
- This vector is normalized. That is $|\alpha|^2 + |\beta|^2 = 1$.
- modulus of α and β : $|\alpha|^2 = (\alpha)(\alpha)^*$ $|\beta|^2=(\beta)(\beta)^*$
- Here * denotes the complex conjugate.

Complex Conjugate and conjugate transpose

- Original matrix M= $\begin{bmatrix} 2+3i & i & 6-4i \\ 7 & 2-3i & -i \end{bmatrix}$

- Complex conjugate = $\begin{bmatrix} 2-3i & -i & 6+4i \\ 7 & 2+3i & i \end{bmatrix}$

- Conjugate Transpose= $\begin{bmatrix} 2-3i & 7 \\ -i & 2+3i \\ 6+4i & i \end{bmatrix}$

Inner products

- inner product between two vectors $|u>$,$|v>$ is represented by using the notation $\langle \boldsymbol{u}|\boldsymbol{v}\rangle$.
- If the inner product between two vectors is zero.$\langle \boldsymbol{u}|\boldsymbol{v}\rangle = \mathbf{0}$ **,** Then

$|u>$ and $|v>$ are ***orthogonal*** to one another.

$$\mathbf{U}=\begin{pmatrix} \boldsymbol{u1} \\ \boldsymbol{u2} \\ \boldsymbol{u3} \end{pmatrix} \quad \mathbf{v}=\begin{pmatrix} \boldsymbol{v1} \\ \boldsymbol{v2} \\ \boldsymbol{v3} \end{pmatrix} \quad \boldsymbol{u}^T\mathbf{v} = \begin{pmatrix} \boldsymbol{u1} & \boldsymbol{u2} & \boldsymbol{u3} \end{pmatrix} \begin{pmatrix} \boldsymbol{v1} \\ \boldsymbol{v2} \\ \boldsymbol{v3} \end{pmatrix} = \boldsymbol{u1v1} + \boldsymbol{u2v2} + \boldsymbol{u3v3}$$

<u>Norm of a vector</u> : $\|u\|=(u^T\ u)^\wedge{}^1/_2$

- If norm of a vector =1 , Then we can say that |U> is normalized.

Outer Product

- outer product of two states $|\psi> = \begin{pmatrix} a \\ b \end{pmatrix}$ and $|\varphi> = \begin{pmatrix} c \\ d \end{pmatrix}$ is represented as,

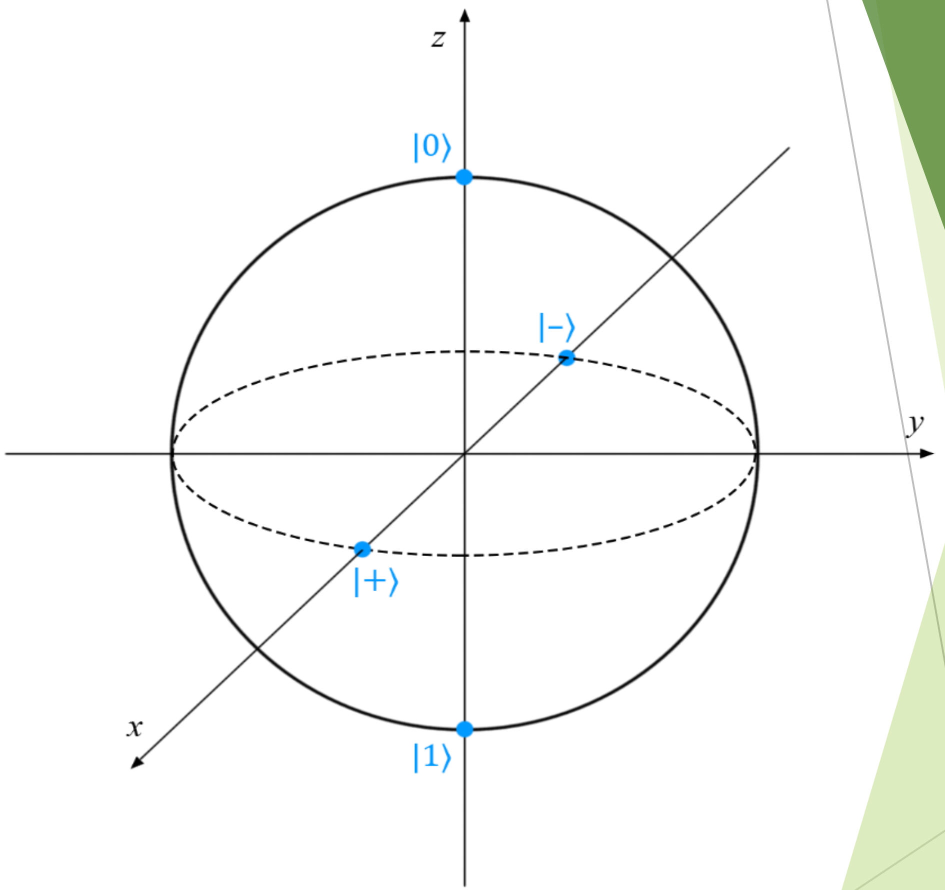
$$|\psi><\varphi| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c* & d* \end{pmatrix} = \begin{pmatrix} ac* & ad* \\ bc* & bd* \end{pmatrix}$$

Orthonormality

- If each elements of vector is normalized and the elements are orthogonal with respect to each other we say the set is orthonormal.
- $\langle 0|0\rangle = (1 \quad 0)\begin{pmatrix}1\\0\end{pmatrix} = 1$
- $\langle 0|1\rangle = (1 \quad 0)\begin{pmatrix}0\\1\end{pmatrix} = 0$
- $\langle 1|0\rangle = (0 \quad 1)\begin{pmatrix}1\\0\end{pmatrix} = 0$
- $\langle 1|1\rangle = (0 \quad 1)\begin{pmatrix}0\\1\end{pmatrix} = 1$
- So $|0>$ and $|1>$ are orthonormal.
- Normalization of state: $|\psi> = \frac{|\psi>}{\sqrt{\langle \psi|\psi\rangle}}$

The Bloch's Sphere

- Bloch's sphere is a geometric representation of quantum states. where different points in the surface of the unit radius sphere represent various quantum state.
- A qubit can be represented in 3D space as a vector of unit length connecting points in the surface of the Bloch's sphere and it's center.
- $|+\rangle = {}^{1}/_{\sqrt{2}}\,(|0\rangle + |1\rangle)$
- $|-\rangle = {}^{1}/_{\sqrt{2}}\,(|0\rangle - |1\rangle)$
- |+> and |-> are called Hadamard's basis.



operations on a single qubit are represented by rotations on this sphere

$$|\psi\rangle = \cos(\tfrac{\theta}{2})\,|0\rangle + e^{i\varphi}\sin(\tfrac{\theta}{2})|1\rangle$$

How to Measure a Qubit ?

Measuring qubits

- Like a bit in classical computer qubits can have values in form of 0 or 1.
- But unlike classical bits it exists in a superposition of states. Which means at that time it has both the values(0 & 1) at the same time.
- When we try to observe the superposition state it collapses to one of the values and it will remain in that state for the rest of the time.
- The collapse of superposition state in in-deterministic and completely random.
- We cannot tell beforehand in which state the superposition collapsed to , but we can find the probability of the superposition state to collapse in one of two states.

- If $|\psi>$ is in a state $|0>$ or Spin Up state

ie, $|\psi> = |\uparrow> = \begin{pmatrix}1\\0\end{pmatrix}$ Then,There is 100% probability $|\psi>$ occurs in Spin Up (|0>) and 0% probability in Spin down(|1>).

- If $|\psi>$ is in a state $|1>$ or Spin Down state

ie, $|\psi> = |\downarrow> = \begin{pmatrix}0\\1\end{pmatrix}$ Then,There is 0% probability $|\psi>$ occurs in Spin Up (|0>) and 100% probability in Spin down(|1>).

- If $|\psi> = \alpha|0> + \beta|1> = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$ Then the probability of $|\psi>$ occurring in state $|0>$ is $|\alpha|^2$ and probability of $|\psi>$ occurring in state $|1>$ is $|\beta|^2$.
- **P0** $= |\langle\psi|0\rangle|^2 = |\alpha|^2$: probability of getting outcome |0>
- **P1** $= |\langle\psi|1\rangle|^2 = |\beta|^2$: probability of getting outcome |1>

$$p_0 = |\langle\psi|0\rangle|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right|^2 = |\alpha|^2,$$

$$p_1 = |\langle\psi|1\rangle|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right|^2 = |\beta|^2.$$

Many Qubits…

Standard Basis for Two Qubits

- $State\ |00>= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$
- $State\ |01>= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$
- $State\ |10>= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$
- $State\ |11>= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Multiple Qubits

- State of Multi-Qubit system obtained by taking tensor product of individual qubit state.

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 \\ 1 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

- te .

Tensor product for two qubits

- The probability vector for two qubit |vw> being in the state |00>, |01>, |10> or |11> is denoted :

$$|v> \otimes |w> = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \otimes \begin{pmatrix}\delta \\ \gamma\end{pmatrix} = \begin{pmatrix}\alpha\delta \\ \alpha\gamma \\ \beta\delta \\ \beta\gamma\end{pmatrix}$$

The probability of |w> being |1> and |v> being |0> is $|\alpha\Upsilon|^2$

- The tensor product is used to combine two qubits.
- **Properties of Tensor Product:**

1. It is Distributive
2. It is Associative
3. Tensor product are not commutative.

The cauchy-Schwartz and Triangle inequalities

- The Cauchy- Schwartz inequalities

$$\langle \psi|\varphi\rangle^2 \leq \langle \psi|\psi\rangle\langle \varphi|\varphi\rangle$$

Absolute value of dot product of two vectors is less than or equal to products of their norms.

- The triangle inequalities

$$\sqrt{\langle \psi+\varphi|\psi+\varphi\rangle} = \sqrt{\langle \psi|\psi\rangle} + \sqrt{\langle \varphi|\varphi\rangle}$$

Matrices and Operators

Matrix representation of operator in 2D Space

- To write the matrix representation of an operator with respect to the computational basis.
- A= $\begin{pmatrix} \langle 0|A|0\rangle & \langle 0|A|1\rangle \\ \langle 1|A|0\rangle & \langle 1|A|1\rangle \end{pmatrix}$
- Example : matrix representation of Z operator .z|0> = |0>, z|1>= -|1>

$$Z= \begin{pmatrix} \langle 0|z|0\rangle & \langle 0|z|1\rangle \\ \langle 1|z|0\rangle & \langle 1|z|1\rangle \end{pmatrix} = \begin{pmatrix} \langle 0|0\rangle & \langle 0|-1\rangle \\ \langle 1|0\rangle & \langle 1|-1\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- An operator transforms vectors into other vectors that belongs to the same space.
- **Pauli Matrices**

Pauli-x $=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Pauli-y $=\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

Pauli-z$=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Identity matrix$=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

- **HERMITIAN MATRICES** : It is a complex square matrix that is equal to it's own conjugate transpose.

$$H^T = H$$

- **UNITARY MATRICES** : A square matrix is called a unitary matrix if it's conjugate transpose is also it's inverse.

$$U^T = U^{-1}$$

Eigen values and Eigen Vectors

- A given vector is said to be an eigenvector of an operator A if the following equation is satisfied, where λ is a complex number:

  A|ψ>=λ|ψ > The number λ is called an eigenvalue of the operator A.

- To find Eigen values we use "Characteristic equation".
- Characteristic equation :det $|A - \lambda I| = 0$
- where λ is an unknown variable, I is the identity matrix and det denotes the determinant of the matrix A−λI. The values of λ that are the solutions to this equation are the eigenvalues of the operator A.
- Determinant of a 2x2 matrix given by det|A|=$\begin{vmatrix} a & b \\ c & d \end{vmatrix}$=ad-cb

Spectral Decomposition

- An operator A belonging to some vector space that is normal and has a diagonal matrix representation with respect to some basis of that vector space. This result is known as the spectral decomposition theorem.
- If operator A satisfies the spectral decomposition theorem for some basis |u>. we can write the operator in the form.

$$A = \sum_{i=1}^{n} a_i |u_i\rangle\langle u_i|$$

- Here ai are the eigen value of the operator A.

The Expectation Value of an Operator

- The expectation value of an operator is the mean or average value of that operator with respect to a given quantum state.
- It is the probabilistic expected value of the result (measurement) of an experiment.
- We write the expectation value as $\langle A \rangle = \langle \psi | A | \psi \rangle$

The trace of an operator

- The trace of an operator is the sum of diagonal elements of a matrix.
- **Tr(M)=** $\sum_{i=1}^{n} \langle \boldsymbol{ui} | \boldsymbol{M} | \boldsymbol{ui} \rangle$
- The trace of an operator is equal to the sum of its eigen values.
- z=$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, Tr(Z)= Tr$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ = 1+(-1) = 0

Positive operator

- An operator A is said to be positive semi-definite

if $\langle \psi | A | \psi \rangle$ >= 0 ,for all |ψ>$\in C^n$.

The Projection operator

- It is an operator that can be formed by writing the outer product using a single ket.
- $P = |\psi >< \psi|$
- It is a Hermitian. If the state |ψ> is normalized. Then a projection operation is equal to it's square.
- $P^2 = P$
- If P1 and P2 are projection operators that commute, meaning that P1P2=P2P1, then their product is also a projection operator.
- By using spectral decomposition we can write the operator A as

 $A = \sum_{i=1}^{n} ai|ui >< ui|$, The projection operator Pi=|ui><ui| projects onto the subspace defined by the eigenvalue ai.

- So we can rewrite the equation as $A = \sum_{i=1}^{n} aipi$
- Completeness of a basis ,we can write I =$\sum pi$

- Basis state |0> and |1>

$$P0 = |0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$$

$$P1 = |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$$

$$P0 + P1 = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = I\,,$$

it satisfy Completeness,

Unitary transformation

- It perform matrix representation from one basis to a representation of that in another basis.

Commutator Algebra

- The commutator of two operator A and B is defined as

$$[A, B] = AB - BA$$

- When $[A, B] = 0$ we can say that the operator A and B is commute.
- If it not commute then they are incompatible.
- Commutator is Antisymmetric meaning $[A, B] = -[B, A]$.
- The commutator is linear means $[A, B + C] = [A, B]+[A, C]$.

Density Matrix

- **Pure state**: Pure state are those for which we can precisely define their quantum state at every point in time.
- A single qubit |q> in state |0> and apply a hadmard gate, the final result will be |+> state.

$$H|0> = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0> + |1>) = |+>$$

- However performing any measurements we can say with 100% certainty that, if our qubit initialization process and our hadmard gate is ideal the resulting state will always |+>.
- An alternate way to express this pure quantum state in form of a matrix, This can be done by using Density operator. $\boldsymbol{\rho = |\psi >< \psi|}$

- **Mixed state** : Those are consist of statistical ensembles of different quantum state.
- Unlike pure states, mixed state cannot be represented as linear superposition of normalized state vectors.
- The mixed state is the combination of probabilities of the information about the quantum state of the quantum system.
- A pure state is the quantum state where we have exact information about the quantum system. And the mixed state is the combination of probabilities of the information about the quantum state. different distributions of pure states can generate equivalent mixed states.
- State generated with some probability : |ψj> with probability Pj the density matrix given by

$$\rho = \sum pj|\psi j >< \psi j|$$

- Consider a Mixed state that contains the combination of pure state

$$|\psi> = |0> \quad or \quad |\psi> = |1> \quad or \quad |\psi> = |0> + |1>$$

We cannot represent it with a wave function .

By using Density Operator we can represent it.

$$|\psi> = |0> = \begin{pmatrix}1\\0\end{pmatrix}, \rho A= \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$$

$$|\psi> = |1> = \begin{pmatrix}0\\1\end{pmatrix}, \rho B= \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$$

$$|\psi> = |0> + |1> = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \rho c=\frac{1}{2} \begin{pmatrix}1\\1\end{pmatrix}\begin{pmatrix}1 & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}$$

$$\rho ABC = \frac{1}{3}(\rho A + \rho B + \rho C) = \frac{1}{3}\left(\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix} + \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}\right)$$

$$= \begin{pmatrix}\frac{1}{2} & \frac{1}{6}\\ \frac{1}{6} & \frac{1}{2}\end{pmatrix}$$

- A mixed sate is represented by a sum of probabilities for finding the system in each state.

- **Density Matrix**: Density matrix is an alternative way of expressing quantum states. However, unlike the state-vector representation, this formalism allows us to use the same mathematical language to describe both the more simple quantum states, as well as the *mixed states* that consist of ensembles of pure states.
- Advantages of density matrix:
- It allows for the calculation of probabilities of the outcome of any measurement performed upon this system using Born' s rule.
- Born's Rule: The probability of each measurement result is given by the corresponding squared amplitudes.
- It is a generalization of the more usual state vectors or wave functions while those can only represent pure states, density matrices can also represent mixed states.

On a Bloch sphere, pure states are represented by a point on the surface of the sphere, whereas mixed states are represented by an interior point. The completely mixed state of a single qubit $\frac{1}{2}$ I2 is represented by the center of the sphere.

Example : Density matrix of a system arising from a process that generate 0 with probability half and 1 with probability half.

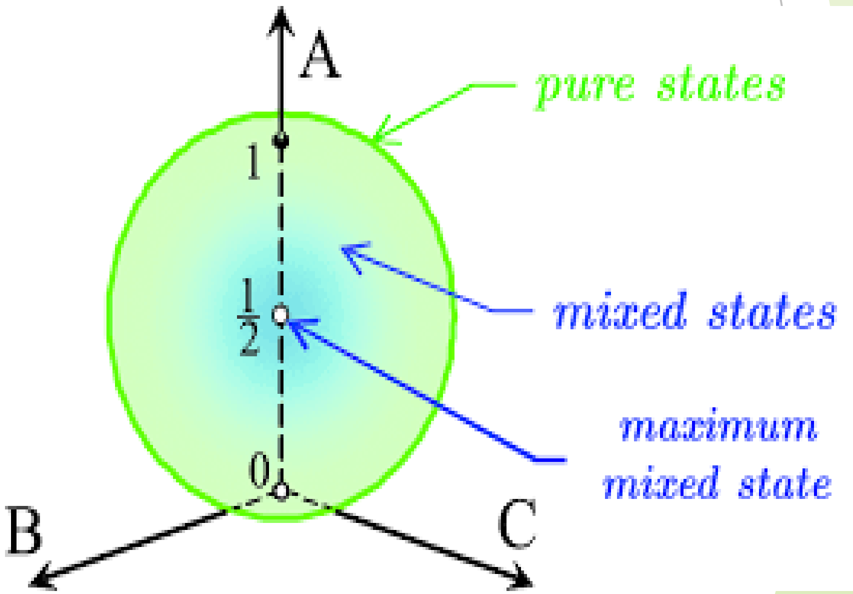
$$\frac{1}{2}|0\rangle = \frac{1}{2}|0\rangle\langle 0| = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

$$\frac{1}{2}|1\rangle = \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

The density matrix $\rho = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$

$$= \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{2}\,\mathrm{I}$$

"ρ " is a mixed state, it is called maximally mixed state.



- A qubit density matrix with Bloch vector $V=(V_x,V_y,V_z)$.
- If $V_x^2 + V_y^2 + V_z^2 <= 1$, then ρ is a valid state.
- If $V_x^2 + V_y^2 + V_z^2 = 1$, then ρ is a pure state.
- If $V_x = V_y = V_z = 0$ (origin), then ρ is maximally mixed state.

Quantum Gates

Single Qubit Quantum Gates

- It is an unitary operations.(u^Tu= I)
- Any single qubit quantum gate is given by an unitary transformation

$$U = e^{i\alpha} Rn\ (\theta)$$

Here R is the rotational operator about an arbitrary direction and n is the unit vector.

Pauli Gates

The Pauli-X gate is a single-qubit rotation through *π(180)* radians around the x-axis. It is work like as a NOT gate in classical computer. It convert state $|0> to\ |1>$ and $|1>$ to $|0>$. It is also called as bit-flip gate.

Pauli x gate outer product form : $\boldsymbol{X = |0><1| + |1><0|}$

Pauli Y Gate

The Pauli Y gate maps $|0> to\ i|1>$ and $|1> to\ -i|0>$. The Pauli−Y gate is a single−qubit rotation through π radians around the y−axis.

Pauli Y Gate outer product form : **Y**$= \boldsymbol{-i|0><1| + i|1><0|}$

Pauli Z Gate

The Z-gate is a unitary gate that acts on only one qubit. Specifically it maps 1 to -1 and leaves 0 unchanged. It does this by rotating around the Z axis of the qubit by π radians (180 degrees). By doing this it flips the phase of the qubit. It is also called Phase flip gate.

Pauli Z gate outer product form : **Z** $=\boldsymbol{|0><0| - |1><1|}$.

- Pauli X gate is not an universal NOT gate.It only operate on single qubit pure state. It is not for the linear combinations.

Hadamard Gate

It create superposition of basis gate.

Outer product form of

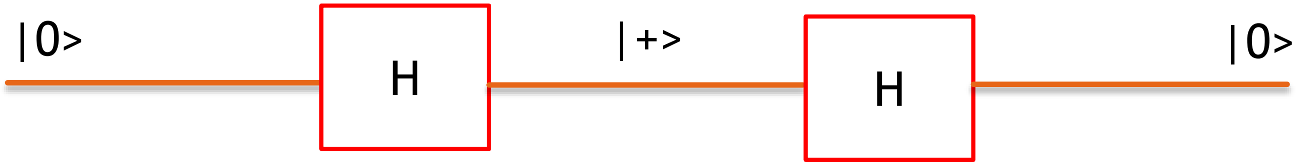
hadamard gate= $\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\mathbf{0}><\mathbf{0}|+|\mathbf{0}><\mathbf{1}|+|\mathbf{1}><\mathbf{0}|-|\mathbf{1}><\mathbf{1}|)$

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

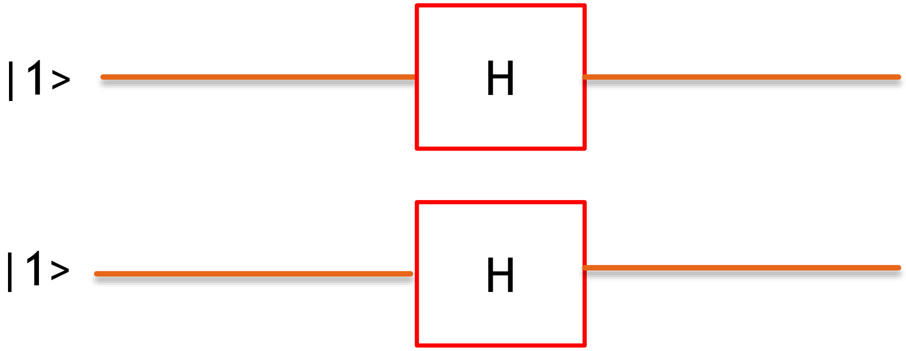
$$H(|1\rangle)=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=|-\rangle$$

- |+> and |-> are called Hadamard basis.
- Hadamard gate is also called as square root of NOT gate($\sqrt{NOT}$).Because it produce states that are lie in the halfway between 0 and 1.

- Hadamard Gate in Series: Two hadamard gate in series restore a qubit to its orginal state.



- Hadamard gate in Parallel : Two hadamard gate in parallel gives the tensor product of two hadamard gate.



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

$$= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)$$

- When “n” hadamard gates act in parallel on “n” qubit is called “Hadamard Transform”.

I S T Gates

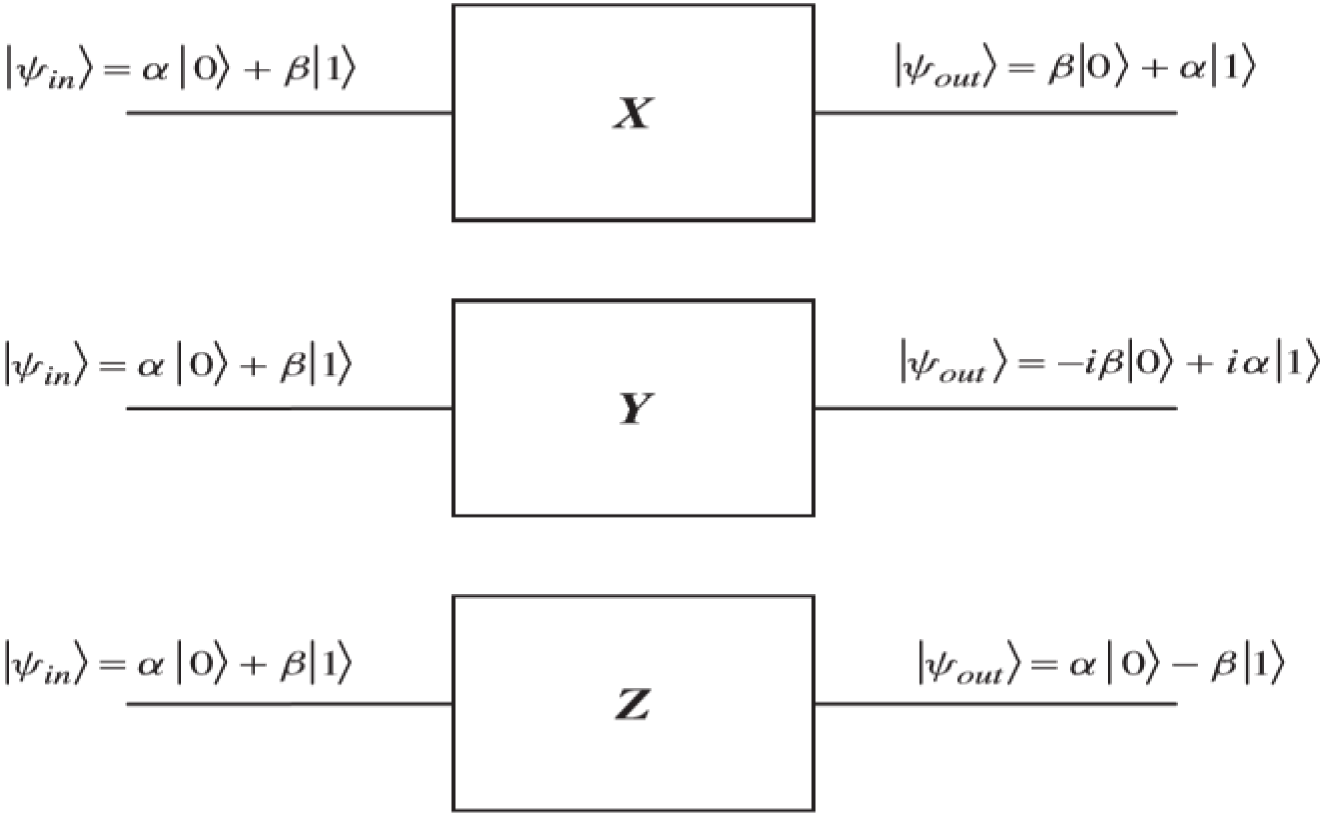
- Rotation about Z axis gives the matrix: $Rz(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$ by adding a global phase($e^{i\theta/2}$)gives us a new form of the matrix. The operation will remains same as the previous one.

  $Rz(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$

- If $\theta = 2\pi$ Then Rz become identity matrix, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- If $\theta = \pi/2$ Then Rz become S matrix ,$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
- If $\theta = \frac{\pi}{4}$ Then Rz become T matrix, T= $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$,it is also called square root of S gate.

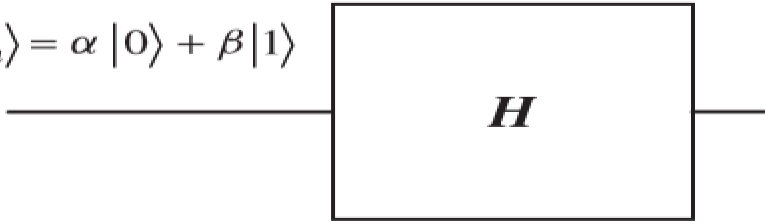
Basic Quantum Circuits

- The Circuit diagram representations of the Pauli operators and their actions on a single arbitrary qubit .



- The Hadamard gate circuit

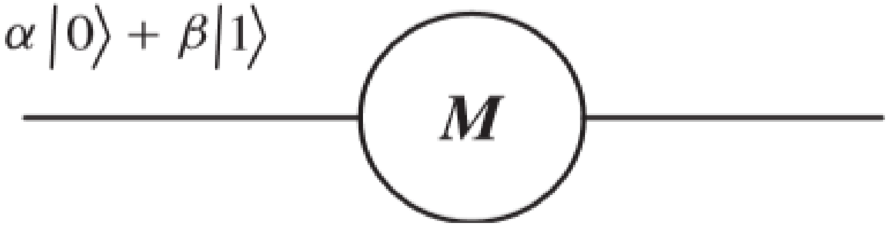
$$|\psi_{in}\rangle = \alpha\,|0\rangle + \beta|1\rangle$$



$$|\psi_{out}\rangle = \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|1\rangle$$
$$= \alpha\,|+\rangle + \beta|-\rangle$$

- Representation of measurement in a quantum circuit

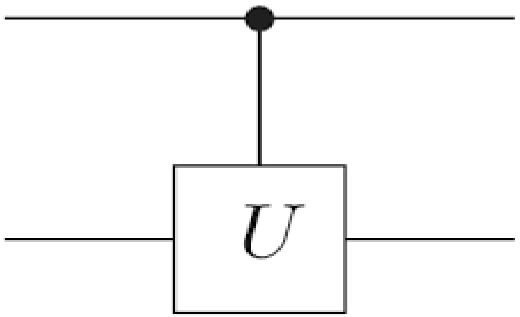
$$|\psi_{in}\rangle = \alpha\,|0\rangle + \beta|1\rangle$$



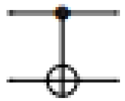
$$P_0 = |\langle 0|\psi\rangle|^2 = |\alpha^2|$$
$$P_1 = |\langle 1|\psi\rangle|^2 = |\beta^2|$$

Two Qubit Quantum Gate

- Two qubit gate is also called "Controlled Unitary Operation (CU)".
- $CU = \begin{bmatrix} I_2 & 0_2 \\ 0_2 & U_2 \end{bmatrix}$

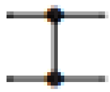


- If U=X=$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ then the Gate will be CNOT.
- **CNOT Gate:** The first bit of a CNOT gate is called the "control bit," and the second the "target bit." The control bit does not change, while the target bit flips if and only if the control bit is 1

CNOT $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ 

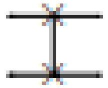
- If $U=Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ then the Gate will be CPHASE Gate.
- **CPHASE Gate**: This gate flips the phase of the target qubit if the control qubit is in the $|1\rangle$ state.

$$\text{CPHASE} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



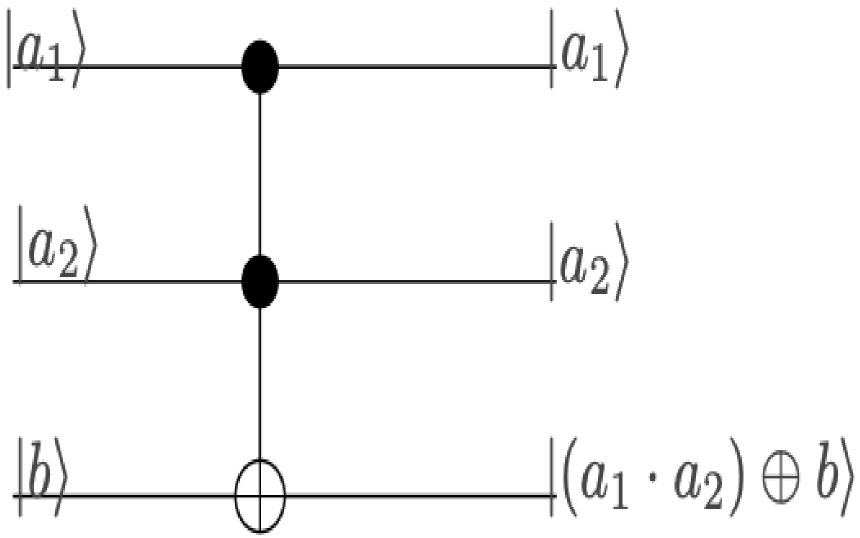
- **SWAP Gate:** The SWAP gate swaps the state of the two qubits involved in the operation

$$\text{SWAP} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



Three Qubit Quantum Gate

- Three Qubit Quantum gate uses “Controlled controlled unitary”(c^2u).
- $\text{Ccu} = c^2u = \begin{bmatrix} I_4 & 0_4 \\ 0_4 & c_u \end{bmatrix}$

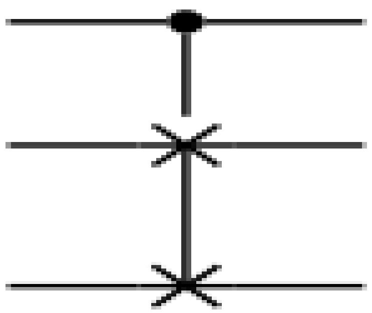


Toffoli Gate:

- Toffoli (Controlled-CNOT) If first qubit is |1>, perform a CNOT on the second and third qubit.
- It has two control bits C1 and C2.
- The gate operates by computing C1 AND C2 ,then compute XOR of the result with a target bit.

Fredkin Gate :

- It has three input. The first of which is a control bit.
- In fredkin gate ,if C=0 then nothing is done to the input bits,they simply pass through the circuit unchanged. If C=1 ,then the values of the bits are interchanged or swapped.

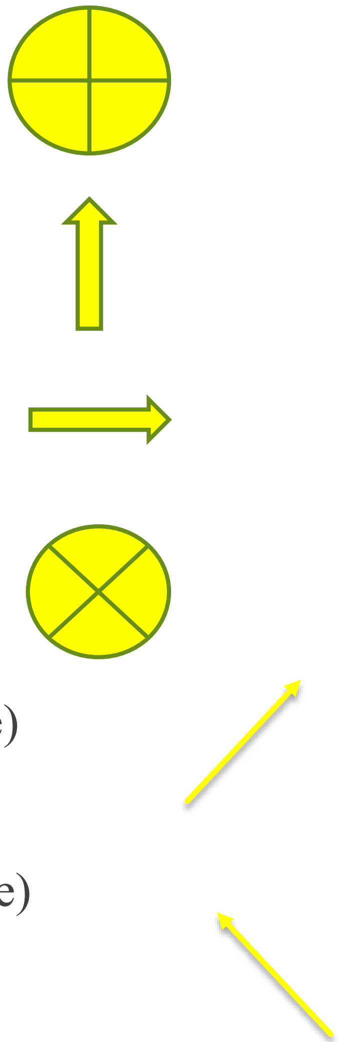


Photon Polarization

- **Photon polarization** is the quantum mechanical description of the classical polarized sinusoidal plane electromagnetic wave.
- An individual photon can be described as having right or left circular polarization, or a superposition of the two.
- Equivalently, a photon can be described as having horizontal or vertical linear polarization, or a superposition of the two.

Types of polarization

- Rectilinear polarization
- Vertical polarization
- Horizontal polarization
- Diagonal Polarization
- Diagonal polarization(45 degree)
- Diagonal polarization(350 degree)

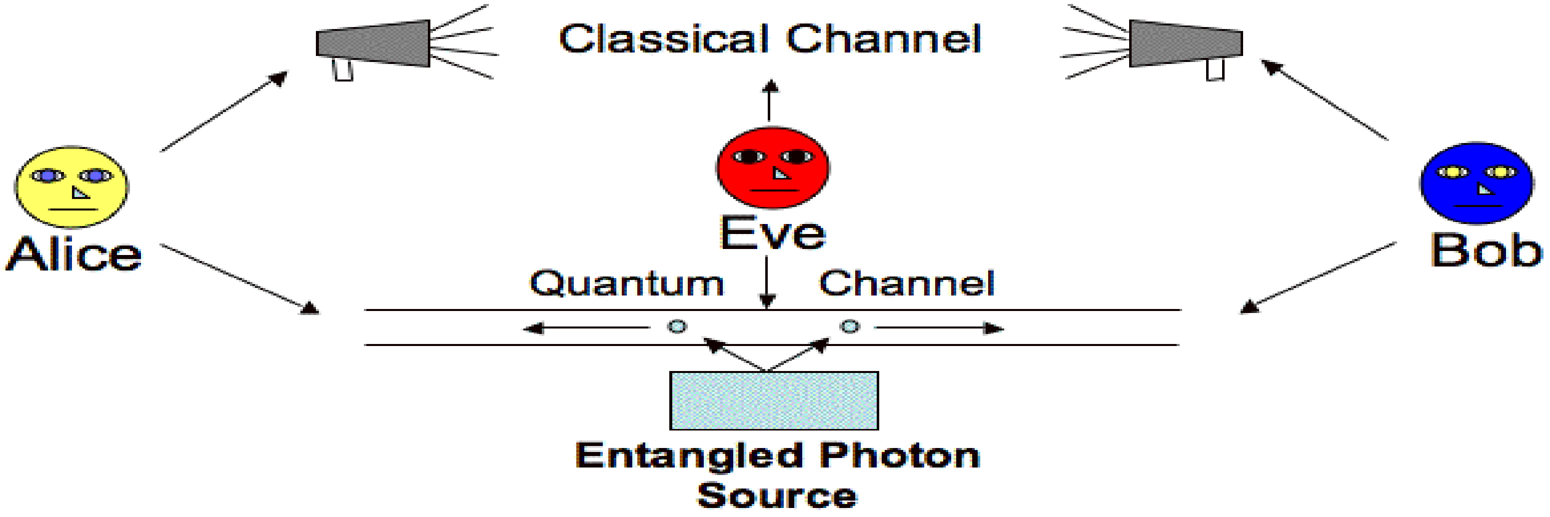


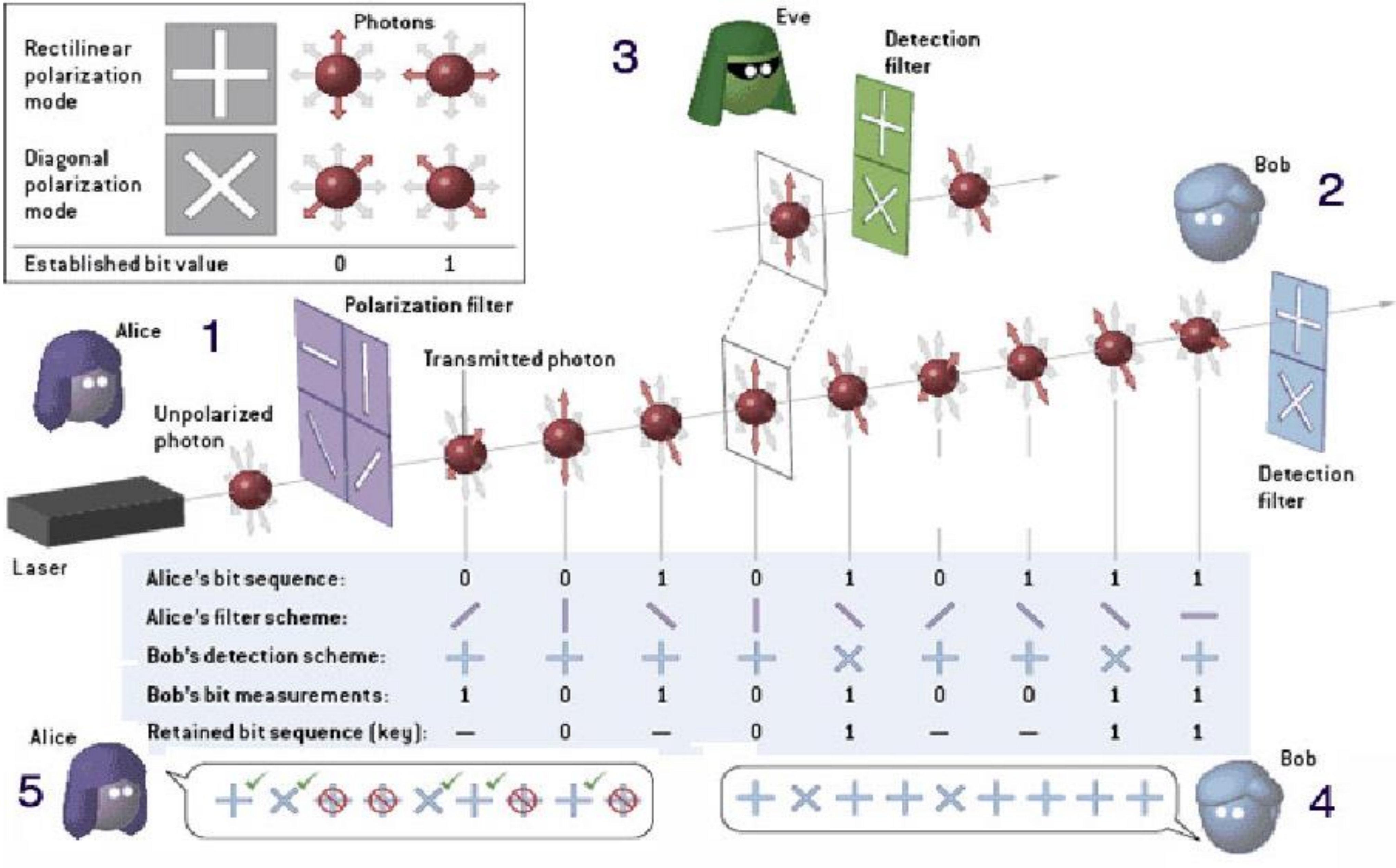
Quantum Key Distribution(QKD)

- This scheme allows the one to distribute the sequence of random bits whose randomness and privacy are guaranteed by the laws and concept of quantum mechanics. These sequences can be used as secret keys and also surety about the confidentiality data transfer.
- There have some practical limitations of quantum key distribution.
- QKD requires an optical environment for transmission like optical fiber.
- The range of QKD is limited about 60 miles or 100 kms.
- Quantum key is only used to produce and distribute key only not for message and any type of data.

BB84 Protocol(Bennett and Brassard)

- In this protocol, The pair of states are used and these pair of states are orthogonal to each other.
- In it Alice chooses a random bit like 0 or 1 then set with the basis, basis are two types one is rectilinear and diagonal basis.
- Alice sends photon in that state to Bob .
- Bob is also randomly go with basis. If bit have same basis correspondingly at both ends then successfully shared key.




Photons
Rectilinear polarization mode
Diagonal polarization mode
Established bit value 0 1
3
Eve
Detection filter
Bob
2
Polarization filter
Alice
1
Transmitted photon
Unpolarized photon
Laser
Detection filter
Alice's bit sequence: 0 0 1 0 1 0 1 1 1
Alice's filter scheme:
Bob's detection scheme:
Bob's bit measurements: 1 0 1 0 1 0 0 1 1
Retained bit sequence (key): – 0 – 0 1 – – 1 1
Alice
5
Bob
4

Quantum Encryption Using One Time Pad

Encryption and Decryption using Classical Bits

- Encryption

e=m XOR k , Where m is the plain text, k is the key and e is the cipher text

- Decryption

m= e XOR k = (m XOR k) XOR k

Encryption and Decryption using Quantum Bits

- Encryption

$$|\boldsymbol{e}> = \boldsymbol{X}^{\boldsymbol{k1}}\boldsymbol{Z}^{\boldsymbol{k2}}|\boldsymbol{m}>$$

- Where |m> is the quantum state to be encrypted.
- *X* is the Quantum NOT gate .It perform Bit-Flip operation on Standard Basis.$\boldsymbol{x}|\boldsymbol{m}> = |\boldsymbol{m}\ \boldsymbol{XOR}\ \boldsymbol{1}>$.
- Z is the Quantum Z gate. It perform Bit-Flip operation on Hadmard basis.$\boldsymbol{Z}|\boldsymbol{m}> = (-\boldsymbol{1})^{\boldsymbol{m}}|\boldsymbol{m}>$

- Decryption

$$|\boldsymbol{m}> = \boldsymbol{Z}^{\boldsymbol{k2}}\boldsymbol{X}^{\boldsymbol{k1}}|\mathrm{e}>=\boldsymbol{Z}^{\boldsymbol{k2}}\boldsymbol{X}^{\boldsymbol{k1}}(\boldsymbol{X}^{\boldsymbol{k1}}\boldsymbol{Z}^{\boldsymbol{k2}}|m>)$$

Combining Multiple Qubits-Tensor product of Density Matrices

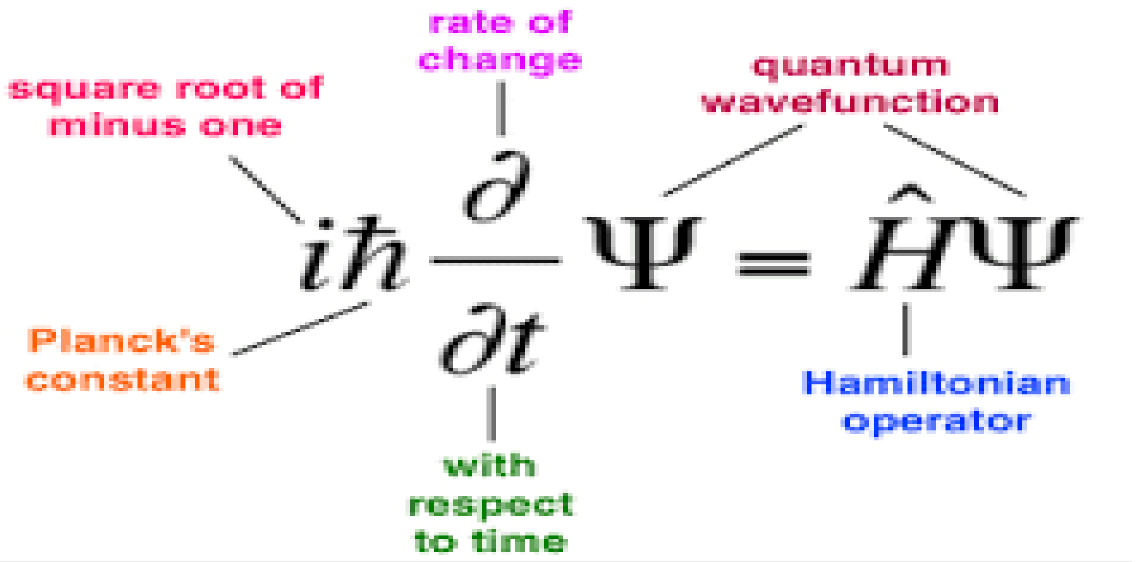
- Two qubits $|\psi A>$ and $|\psi B>$ the density matrix of A and B given by

  $$\rho A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \rho B=\begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

- $|\psi AB>$ join state of two qubits using tensor product = $|\psi A> \otimes |\psi B>$
- $\rho AB = \rho A \otimes \rho B$

Schrodinger's Equation

- The **Schrödinger equation** is a linear partial differential equation that governs the wave function(Mathematical description) of a quantum-mechanical system.



- The **Hamiltonian** of a system is an operator corresponding to the total energy of that system, including both kinetic energy and potential energy.

Quantum Interference

- The application of a hadamard gate to an arbitrary qubit is an example of quantum interference.

Ex: When we calculate H|ψ> for $|\psi> = \alpha|0> + \beta|1>$.

Then, H|ψ> = $\left(\frac{\alpha+\beta}{\sqrt{2}}\right)$|0> + $\left(\frac{\alpha-\beta}{\sqrt{2}}\right)$|1>.

- The probability of to obtain |0> upon measurement has been changed as

  α *to* $\left(\frac{\alpha+\beta}{\sqrt{2}}\right)$.

- The probability of to obtain |0> upon measurement has been changed as

  β *to* $\left(\frac{\alpha-\beta}{\sqrt{2}}\right)$.

There are two types of interference,

- **Positive Interference** in which probability amplitudes add constructively to increase or **Negative interference** in which the probability amplitudes destructively to decrease.

Classical Quantum State

When a authority holding some classical information and a evesdropper holds some quantum information , the joint state of classical and quantum information is called **classical quantum state.**

- **Classical State:** A system X is in a classical state or a c-state, when the corresponding density matrix ρx is diagonal in the standard basis of the state space of x.

$$\rho = \sum px|x >< x|$$

- A classical quantum state or simply called cq-state takes the form,

$$\rho x Q = \sum p x | x >< x |_x \, p_x \mathrm{Q}$$

It consist of a classical register x and a quantum register Q.