Basic concepts of complex NO.

A complex NO. is any NO. of the form

$z = a + bi$

a : real part — bi : Imaginary part

$Re(z) = a$ — $Im(z) = b$

i is imaginary unit NO. $\quad i = \sqrt{-1}$

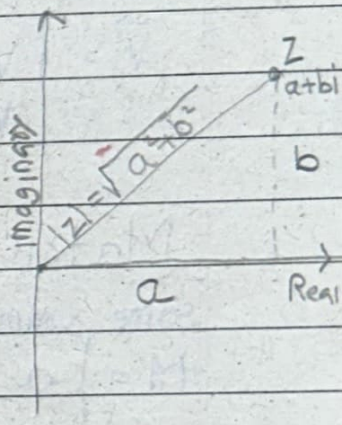
Complex conjugate

$z = a + bi$ $\qquad \bar{z} = a - bi$

Modulus:

$|z| = \sqrt{a^2 + b^2}$

Using distance formula from origin



$$z\bar{z} = (a+bi)(a-bi)$$
$$= a^2 + abi - abi + (-i)b^2$$
$$= a^2 + b^2$$
$$= |z|^2$$
$$= |z| = \sqrt{z\bar{z}}$$

Polar form of Complex NO.: Any complex NO. $z = a + bi$ can be written in the form

$z = |z| e^{i\theta}$ where $e^{i\theta} = \cos\theta + i \sin\theta$

$a = |z| \cos\theta$

$b = |z| \sin\theta$

$a + bi = |z| \cos\theta + i|z| \sin\theta = |z| \{\cos\theta + i \sin\theta\}$

$= |z| e^{i\theta}$

Vectors A vector is column of numbers. For example, a 2-dimensional vector looks like

$$\vec{V} = \begin{Bmatrix} V_1 \\ V_2 \end{Bmatrix}$$

n dimension vector $\begin{Bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{Bmatrix}$

Vector Addition: Adding vectors is easy, just add each corresponding components.

$$\vec{V_2} = \begin{bmatrix} V_1 \\ V_2 \end{bmatrix} \qquad \vec{W_2} = \begin{bmatrix} W_1 \\ W_2 \end{bmatrix}$$

$$\vec{V} + \vec{W} = \begin{bmatrix} V_1 + W_1 \\ V_2 + W_2 \end{bmatrix}$$

Vector scalar Multiplication: You can scale a vector by ~~adjusting~~ multiplying each entry by the scalar (the number). if we have

$$\vec{V} = \begin{bmatrix} V_1 \\ V_2 \end{bmatrix} \quad \text{then} \quad c\vec{V} = \begin{bmatrix} cV_1 \\ cV_2 \end{bmatrix}$$

Matricies A matrix is a box of NOs (real or complex)

some examples are

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad N = \begin{bmatrix} 3 & 3 & -1+2i \\ 1 & -3 & 0 \end{bmatrix}$$

Conjugate of a matrix

$$M_1 = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix} \qquad \overline{M} = \begin{bmatrix} 1 & -6i \\ -3i & 2-4i \end{bmatrix}$$

Matrix Transpose

$$M^T = \begin{bmatrix} 1 & 3i \\ 6i & 2+4i \end{bmatrix}$$

Conjugate Transpose of a Matrix

The conjugate transpose of a Matrix M, denoted M^+ ("M dagger")

$$M^+ = \overline{(M^T)}$$

$$M = \begin{bmatrix} 1 & 6 \\ 3i & 2+4i \end{bmatrix} \qquad M^+ = \begin{bmatrix} 1 & -3i \\ -6i & 2-4i \end{bmatrix}$$

Inner Product: To take the inner product of two vectors,
first take the complex conjugate of the first vector, then multiply each of the corresponding NOs in both vectors and then add everything

$$\vec{V} \cdot \vec{W} = \sum_{j=1}^{n} \overline{V_j} W_j$$

$$\vec{V} = \begin{bmatrix} V_1 \\ V_2 \\ \vdots \\ V_n \end{bmatrix} \qquad \vec{W} = \begin{bmatrix} W_1 \\ W_2 \\ \vdots \\ W_n \end{bmatrix}$$

The inner product of $\vec{V}$ & $\vec{W}$ gives
$\vec{V} \cdot \vec{W} = \overline{V_1} W_1 + \overline{V_2} W_2 + \ldots + \overline{V_n} W_n$

It is same as doing matrix multiplication of $\vec{V}^+$ and $\vec{W}$

Hilbert Space: A vector-space with well-defined inner product is called Hilbert Space

Orthogonal Vectors If inner product is 0

eg)

$$\vec{V} = \begin{bmatrix} i \\ i \end{bmatrix} \qquad \vec{W} = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

$$\vec{V}^+ \vec{W} = \begin{bmatrix} -i & -i \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = (-i)1 + (-i)(-1) = 0$$

Norm of Vector: √Inner product with itself

$$\|\vec{v}\| = \sqrt{\vec{v} \cdot \vec{v}}$$

$$= \sqrt{\vec{v}^{+}\vec{v}}$$

$$= \sqrt{|v_1|^2 + |v_2|^2 + \dots + |v_n|^2}$$

$$\|v\| = \sqrt{1^2 + |(-2)^2| + |i|^2} \qquad v = \begin{bmatrix} 1 \\ -2 \\ i \end{bmatrix}$$

$$= \sqrt{6}$$

Unit vectors & Normalization:

Unit vectors: have norm equal to One.

Normalizing a nonzero vector $\vec{v}$ means to scale by $\frac{1}{\|v\|}$ to make it have unit length

$$\left\| \frac{\vec{v}}{\|\vec{v}\|} \right\| = 1$$

Normalizing vector.

$$v = \begin{bmatrix} 1 \\ -2 \end{bmatrix} \qquad |v| = \sqrt{1+4} = \sqrt{5}$$

$$\frac{\vec{v}}{\|v\|} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 \\ -2 \end{bmatrix}$$

Tensor product: The tensor product is a

$$\vec{v} \otimes \vec{w} = \begin{bmatrix} v_1 \\ w_1 \end{bmatrix} \otimes \begin{bmatrix} v_2 \\ w_2 \end{bmatrix} = \begin{bmatrix} v_1 \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \\ v_2 \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} v_1 w_1 \\ v_1 w_2 \\ v_2 w_1 \\ v_2 w_2 \end{bmatrix}$$

Bracket Notation ($\langle | \rangle$)

Defination: The "Ket": When using a vector $\vec{v}$ to represent a quantum state.
we will use a different notation known as "ket", written $|v\rangle$ ("ket v")
This is a notation commonly used in quantum mechanic & doesn't change the nature of the vectors at all.
That is both notations below are equivalent

$$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \longleftrightarrow \vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

Definition: The "bra". The conjugate transpose of a "ket" $|v\rangle$ denoted by

$$\langle v| = (|v\rangle)^+$$

$\langle v|$ is called "bra v"

Example: if $|v\rangle = \begin{bmatrix} 1 \\ i \end{bmatrix}$ then $\langle v| = [1 \; -i]$

- Defination: The "braket". Given two vector $|v\rangle$ and $|w\rangle$, we use the ~~follow~~ following notation for the inner product

$\langle v|w\rangle = |v\rangle \cdot |w\rangle$

$\langle v|w\rangle$ is known as braeket of $|v\rangle$ and $|\vec{w}\rangle$

Observation: Complex conjugate of a braket: If you recall one of the properties of the inner product namely,

~~$\vec{v} \cdot \vec{w} = \overline{\vec{w} \cdot \vec{v}}$~~

$\vec{v} \cdot \vec{w} = \overline{\vec{w} \cdot \vec{v}}$ you can readily see that

$\overline{\langle w|v\rangle} = \langle v|w\rangle$

Braket Notation

Example: Calculate the inner product of

$|V\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ i\end{bmatrix}$ and $|W\rangle = \frac{i}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}$

The inner product of $|V\rangle$ and $|W\rangle$ given by

$$\langle V|W\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & -i\end{bmatrix}\frac{i}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{i(1-i)}{2} = \frac{1+i}{2}$$

Similarly $\langle W|V\rangle = \frac{1-i}{2}$

Hence $\langle W|V\rangle = \overline{\langle V|W\rangle}$

Quantum Bits or Qubits

Definition: (One Qubit)

A qubit is a unit vector in the two dimensional complex vector space.

The two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$

These states ~~are~~ denote as

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

$$\langle 0| = \begin{bmatrix}1, 0\end{bmatrix} \qquad \langle 1| = \begin{bmatrix}0 & 1\end{bmatrix}$$

These vectors physically mean depend on physical realization employed by quantum computing

If we use the energy of an e^- in an atom as our quantum bit, we could say that the ground state (lowest energy) quantum 0 & higher energy in our quantum 1

$$\text{ground} \leftrightarrow |0\rangle = \begin{bmatrix}1\\ 0\end{bmatrix} \qquad \text{excited} \leftrightarrow |1\rangle = \begin{bmatrix}0\\ 1\end{bmatrix}$$

$|0\rangle \equiv |\updownarrow\rangle$ vertically polarized proton
$|1\rangle \equiv |\leftrightarrow\rangle$ horizontally polarized proton

Quantum mechanics: describes the behavior of system as e^-, atoms, molecules photons, even non-sale electrical circuits.
We use mathematics to module these phenomena

Physical Support	Information Support	$\|0\rangle$	$\|1\rangle$
atom	Energy	lowest Energy	Highest Energy
photon	Electro polarization	vertical polarization ↕	Horizontal Polarization ↔
Electron	Electron spin	Up spin ↑	Down Spin ↓

Postulates of Quantum Mechanics

There are four postulates to quantum mechanics which will form basis of Quantum computers
- Postulate 1: Defination of quantum bit, or qubit
- Postulate 2: How qubit(s) transform (evolve)
- Postulate 3: The effect of measurement
- Postulate 4: How qubits combine together
- ~~Postulate 5~~: into system of qubit.

Quantum Bits or Qubits

A generic qubit: A generic qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$
where coefficient α & β are complex numbers and obey the constrain
$|\alpha|^2 + |\beta|^2 = 1$

- When we measure qubit $|\Psi\rangle$ we get 0 $|\alpha|^2 (P(0) = |\alpha|^2)$ or 1 $|\beta|^2 (P(1) = |\beta|^2)$.

The state after measurement $|0'\rangle|1\rangle$

Example: Is the qubit $|\psi\rangle = \frac{3i}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$ is valid?

$$|\psi\rangle = \frac{3i}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = \frac{9}{5} + \frac{1}{5} = \frac{10}{5} = 2 \neq 1$$

The valid qubit is obtained by multiplying $\frac{1}{\sqrt{2}}$,

$$\frac{1}{\sqrt{2}}\frac{3i}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{2}}\frac{1}{\sqrt{5}}|1\rangle$$

Express the following qubit state in the vector form

$$|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle = \frac{1}{\sqrt{5}}\left[\begin{bmatrix}1\\0\end{bmatrix} + 2\begin{bmatrix}0\\1\end{bmatrix}\right] = \frac{1}{\sqrt{5}}\begin{bmatrix}1\\2\end{bmatrix}$$

2. $$\frac{1}{\sqrt{2}}\begin{bmatrix}i\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}\left[i\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\right) = \frac{1}{\sqrt{2}}[i|0\rangle - |1\rangle]$$

3. Compute the bra state associated with the following state $|\psi\rangle$

Write the result in the vector form

$$|\psi\rangle = \frac{2}{\sqrt{7}}|0\rangle + i\sqrt{\frac{3}{7}}|1\rangle$$

$$\langle\psi| = \frac{2}{\sqrt{7}}\langle 0| - i\sqrt{\frac{3}{7}}\langle 1| = \frac{2}{\sqrt{7}}[1\ 0] - i\sqrt{\frac{3}{7}}[0\ 1]$$

$$= \left[\frac{2}{\sqrt{7}} + i\sqrt{\frac{3}{7}}\right]$$

Problems

4. Suppose $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Compute $\langle\psi|\phi\rangle$ and $\langle\phi|\psi\rangle$

$$\langle\psi| = \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) = \frac{1}{\sqrt{2}}([1\ 0] + [0\ 1]) = \frac{1}{\sqrt{2}}[1\ 1$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\right] = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\right] = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

$$\langle\psi|\phi\rangle = \frac{1}{2}\left[[1\ 1]\begin{bmatrix}1\\-1\end{bmatrix}\right] = \frac{1}{2}(1-1) = 0$$

5) What are the probabilities that a measurement will yield 0 or 1 for the following state

$$|\psi\rangle = \frac{1-i}{\sqrt{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle$$

$$P(0) = \frac{|(1-i)|^2}{(\sqrt{3})^2} = \frac{1^2 - 2i + i^2}{3} = \frac{2-2i}{3}$$

$$P(1) = \left(\frac{1}{\sqrt{3}}\right)^2 = \frac{1}{3}$$

Multi Qubit

Two Qubit System

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = 1\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}$$

$$0\begin{bmatrix}1\\0\end{bmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \qquad |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

$\langle 00| = [1\,0\,0\,0]$
$\langle 01| = [0\,1\,0\,0]$
$\langle 10| = [0\,0\,1\,0]$
$\langle 11| = [0\,0\,0\,1]$

Two qubit system

- Consider two generic qubits $(\alpha_1|0\rangle + \beta_1|1\rangle)$ & $(\alpha_2|0\rangle + \beta_2|1\rangle)$

Tensor product

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

$$= \alpha_1\alpha_2\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \alpha_1\beta_2\begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \beta_1\alpha_2\begin{bmatrix}0\\0\\1\\0\end{bmatrix} + \beta_1\beta_2\begin{bmatrix}0\\0\\0\\1\end{bmatrix} = \begin{bmatrix}\alpha_1\alpha_2\\\alpha_1\beta_2\\\beta_1\alpha_2\\\beta_1\beta_2\end{bmatrix}$$

Two-qubit measurement

Consider generic two qubit quantum state
$|\psi\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$

where $\alpha_1\alpha_2, \alpha_1\beta_2, \beta_1\alpha_2, \beta_1\beta_2$ are comple NO. and obey the constraints
$|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 + |\beta_1\alpha_2|^2 + |\beta_1\beta_2|^2 = 1$

After measuring $|\psi\rangle$ we get
00 with probability $|\alpha_1\alpha_2|^2$ or $P(00)$
01 with probability $|\alpha_1\beta_2|^2$ $P(01)$
10 with probability $|\beta_1\alpha_2|^2$ $P(10)$
11 with probability $|\beta_1\beta_2|^2$ $P(11)$

Entangled State
Bell State
EPR pair [Einstein, Podolsky & Rosen]

Defination: A two qubit quauntum state that can not be written as the tensor produc of single qubit quantum state is called entangled quantum state

Example: Consider the two qubit quantum state
$|\psi\rangle = (\gamma_1|00\rangle + \gamma_2|11\rangle)$
with $\gamma_1 \neq 0$ & $\gamma_2 \neq 0$. This can not be written as
$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$

An important two qubit entangled state

$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

The vast majority of quantum state are entangled

Q1 Show that $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ is not an entangled state

$|\psi\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$

Assume that $|\psi\rangle$ is not an entangled state

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$$

$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

$\alpha_1\alpha_2 = 1/\sqrt{2}$

$\alpha_1\beta_2 = 0$

$\beta_1\alpha_2 = 0$

$\beta_1\beta_2 = 1/\sqrt{2}$

#Contradition

Q2 Prove that $|\psi\rangle = \frac{|00\rangle + |01\rangle}{\sqrt{2}}$ is not entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix}\right] = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}1\\1\end{bmatrix}\right]$$

$$= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix} \otimes \left\{\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\right\}\right]$$

$$= \frac{1}{\sqrt{2}}[|0\rangle \otimes [|0\rangle + |1\rangle]]$$

Measuring composite states

$|\psi\rangle = \alpha_1\alpha_2|\theta$

Inverse of a Matrix

$$AA^{-1} = I$$

Transpose of a Matrix

rows $\longleftrightarrow$ col

$$\begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}^T = \begin{bmatrix} 0 & 3 \\ 2 & 1 \end{bmatrix}$$

Complex ~~adjoint~~ conjugate

$$\begin{bmatrix} 2+5i & i \\ 3 & 3-4i \end{bmatrix}^* = \begin{bmatrix} 2-5i & -i \\ 3 & 3+4i \end{bmatrix}$$

Adjoint [Transpose + complex conjugate]

$$X^+ = (X^*)^T$$

$$\begin{bmatrix} 2+5i & i \\ 3 & 3-4i \end{bmatrix}^+ = \begin{bmatrix} 2-5i & 3 \\ -i & 3+4i \end{bmatrix}$$

Unitary Matrix

If $X^+ = X^{-1}$

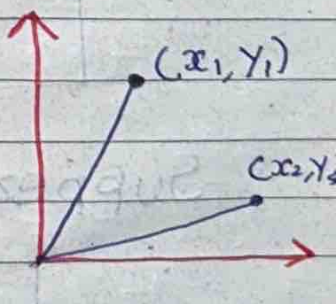
Hermitian Matrix

$X^+ = X$

Linear transformation

$$x_2 = AX_1 + BY_1$$
$$Y_2 = CX_1 + DY_1$$

$$\begin{bmatrix} X_2 \\ Y_2 \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} X_1 \\ Y_1 \end{bmatrix}$$

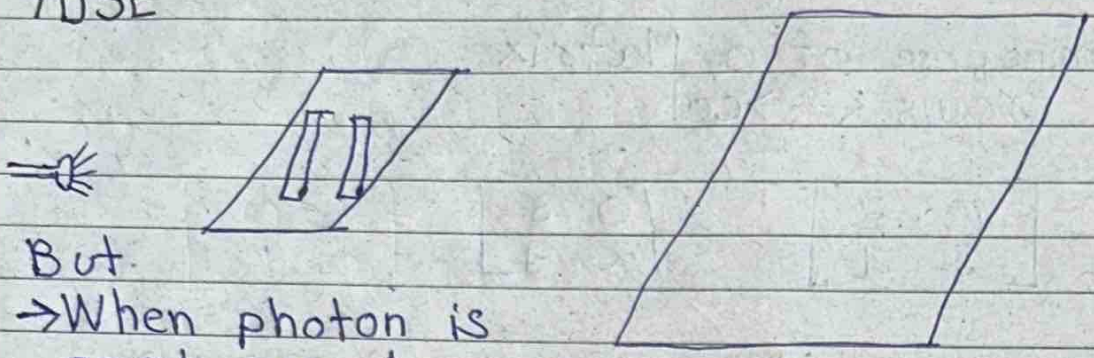


~~Qubit~~ rotation

$$\begin{bmatrix} 0.7 \\ 0.7 \end{bmatrix} = \begin{bmatrix} \cos 45 & -\sin 45 \\ \sin(45) & \cos(45) \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Introduction

YDSE



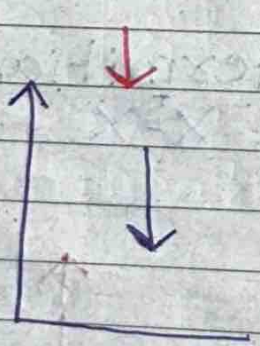
But

→When photon is sent one by one interference pattern takes place

The photon is in the left and right slit at same time

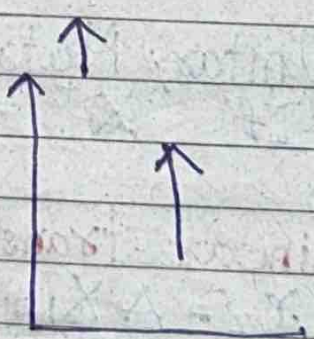
Spin down = 1
Spin Up = 0

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$



Spin down = 0
Spin Up = 1

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$



Supperposition + Entanglemat

$$\begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}$$

$P(00) = 1/2$

$P(11) = 1/2$

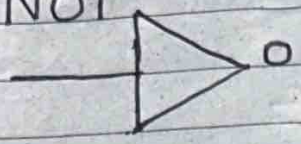
$p = a + bi$

$|p| = a^2 + b^2$

$|p^2| + |q|^2 = 1$

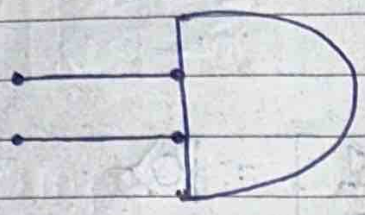
Clasical cate

NOT



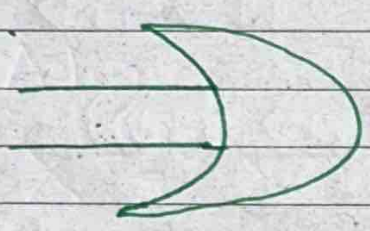
A	O
0	1
1	0

And gate



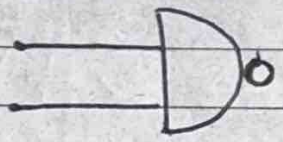
A	B	O
0	0	0
0	1	0
1	0	0
1	1	1

OR gate



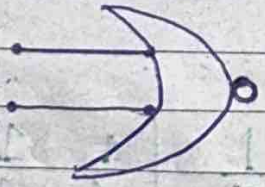
A	B	O
0	0	0
0	1	1
1	0	1
1	1	1

NAND



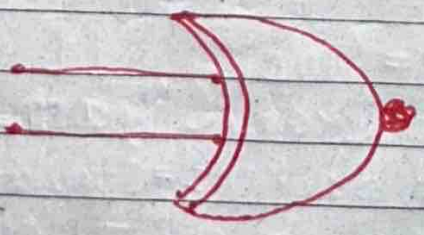
A	B	O
0	0	1
0	1	1
1	0	1
1	1	0

NOR gate



A	B	O
0	0	1
0	1	0
1	0	0
1	1	0

X OR gate



A	B	O
0	0	0
0	1	1
1	0	1
1	1	0

Quantum gate

X gate

aka NOT gate

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

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

Y gate (Pauli's)

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

Z Gate

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

Hadamard Gate

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

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

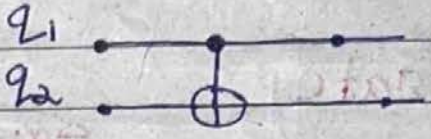
CNOT gate

control not gate

CNOT

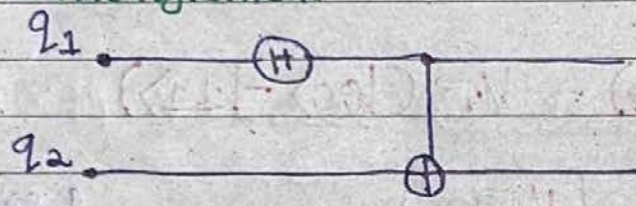
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$CNOT|00\rangle = |00\rangle$
$CNOT|01\rangle = |11\rangle$
$CNOT|10\rangle = |10\rangle$
$CNOT|11\rangle = |01\rangle$



if a,b is qubit
X gate is applied on a
only if b = 1

Entanglement



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

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} * \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

Hadamar gate puts 1 qubit in superposition

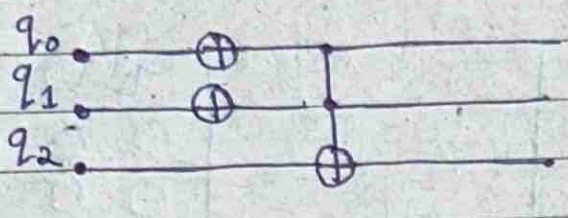
$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \times \begin{bmatrix} 1/\sqrt{2} \\ \\ 1/\sqrt{2} \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \\ 0 \end{bmatrix}$$

Now apply CNOT gate

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}$$

Toffoli gate

2 control bit & 1 tar bit



If q_1 & q_0 are 1 then not gate o q_2

Z gate

equ to phase flip

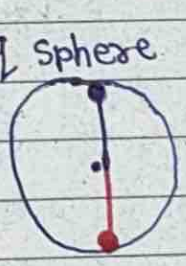
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

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

$Z\left(1/\sqrt{2}\ |00\rangle + |11\rangle\right) = 1/\sqrt{2}\left(|00\rangle - |11\rangle\right)$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} * \begin{bmatrix} 1/\sqrt{2} \\ \\ \\ 1/\sqrt{2} \end{bmatrix}$$

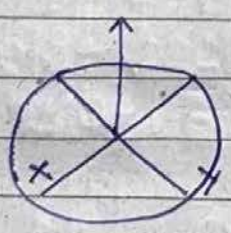


How to create a circuit

```
from qiskit.visualization import plot_histogram
from qiskit import *
circuit = QuantumCircuit(2, 2)
    #quantum_register = QuantumRegister(2)
    #classical_register = ClassicalRegister(2)
    #circuit = QuantumCircuit(quantum_register, classical
circuit.draw()
% matplotlib inline
circuit.draw(output='mpl')
simulator = Aer.get_backend('qasm_simulator')
result = execute(circuit, backend=simulator).result()
plot_histogram(result.get_counts(circuit))
```

To notice phase change
look at bloch sphere

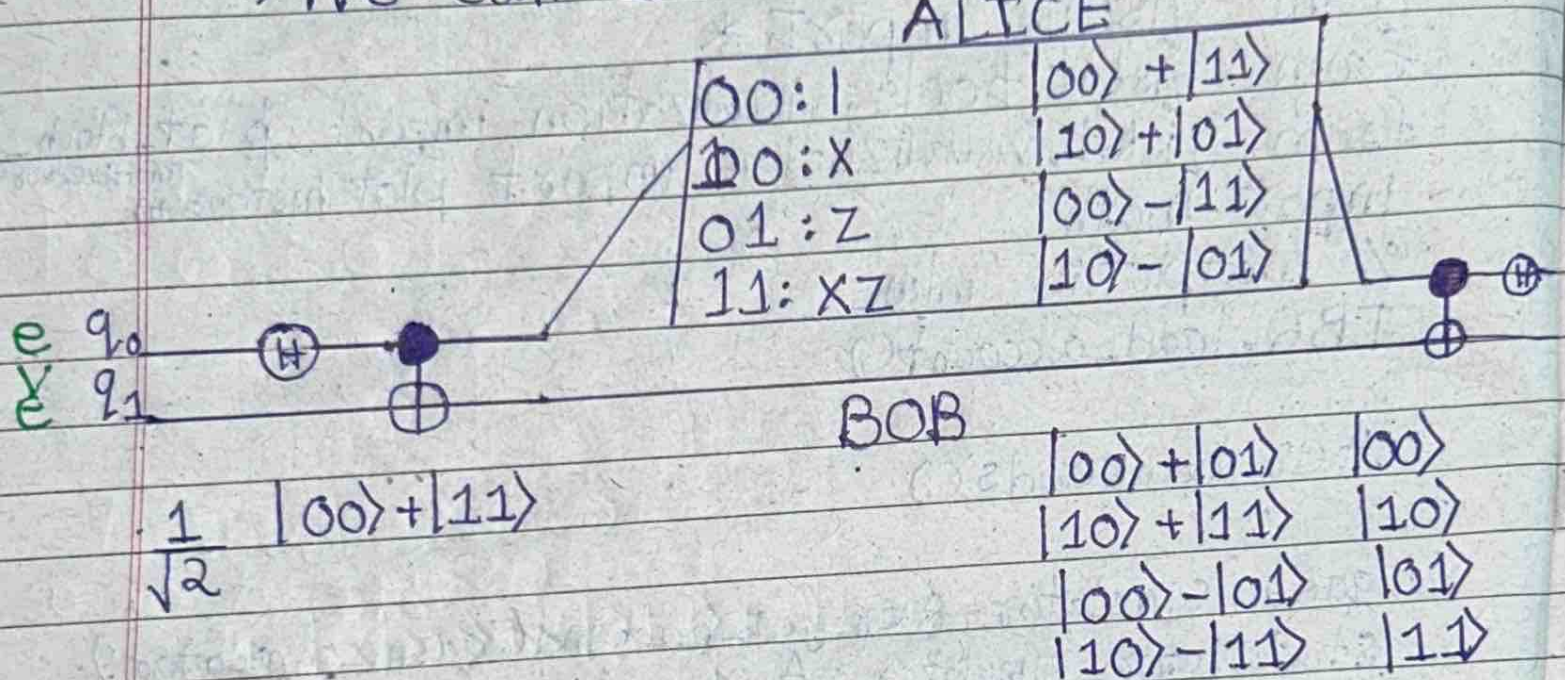
```
from qiskit import *
from qiskit.tools.visualization import plot_bloch_multivector
from qiskit.visualization import plot_histogram
import math
% matplotlib inline
IBQ.load_account()

Aer.backends()

qasm_simulator = Aer.get_backend('qasm_simulator')
statevector_simulator = Aer.get_backend('statevector_
                                        simulator')

def run_on_simulators(circuit):
    statevec_job = execute(circuit, backend=statevector_
                           simulator)
    result = statevec_job.result()
    statevec = result.get_statevector()
    num_qubits = circuit.num_qubits
    circuit.measure([i for in range(num_qubits)]
                    [ifor i in range(num_qubits)]
    qsam_job = execute(circuit, backend=
                       qsam_simulator, shots=1024)
    counts = qsam_job.get_counts()
    return statevec, counts
```



|1⟩

Super dence coding

→ We can store 2 bits using 1 qubit



$\frac{1}{\sqrt{2}}$ $|00\rangle + |11\rangle$

$\|00\rangle + \|01\rangle$	$\|00\rangle$
$\|10\rangle + \|11\rangle$	$\|10\rangle$
$\|00\rangle - \|01\rangle$	$\|01\rangle$
$\|10\rangle - \|11\rangle$	$\|11\rangle$

eve, gives one qubit to ALICE
one qubit to BOB

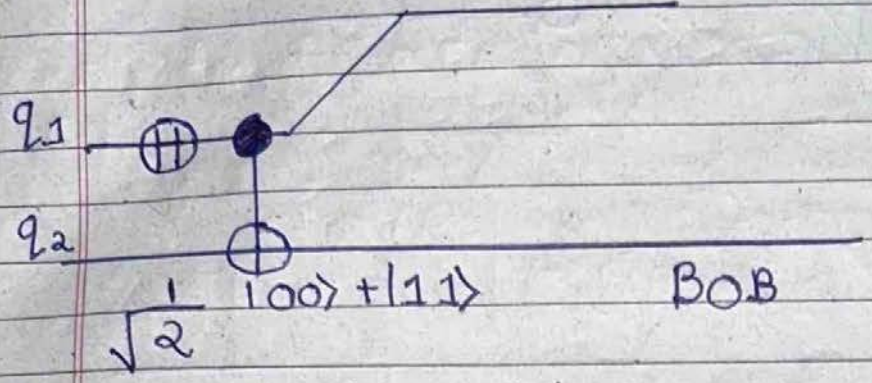
Now ALICE will perform some opperation

Bob will apply CNOT gate & H

The value will change for Bob to

Quantum Teleportation

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

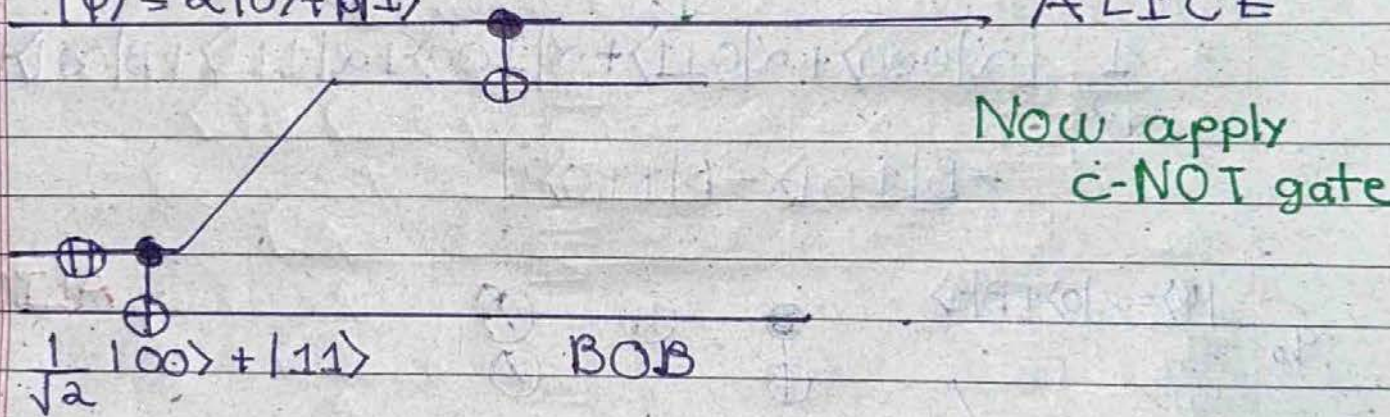


$\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ BOB

Total Quantum state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \otimes \frac{1}{\sqrt{2}}|00\rangle + |11\rangle$$

$$= \frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle]$$

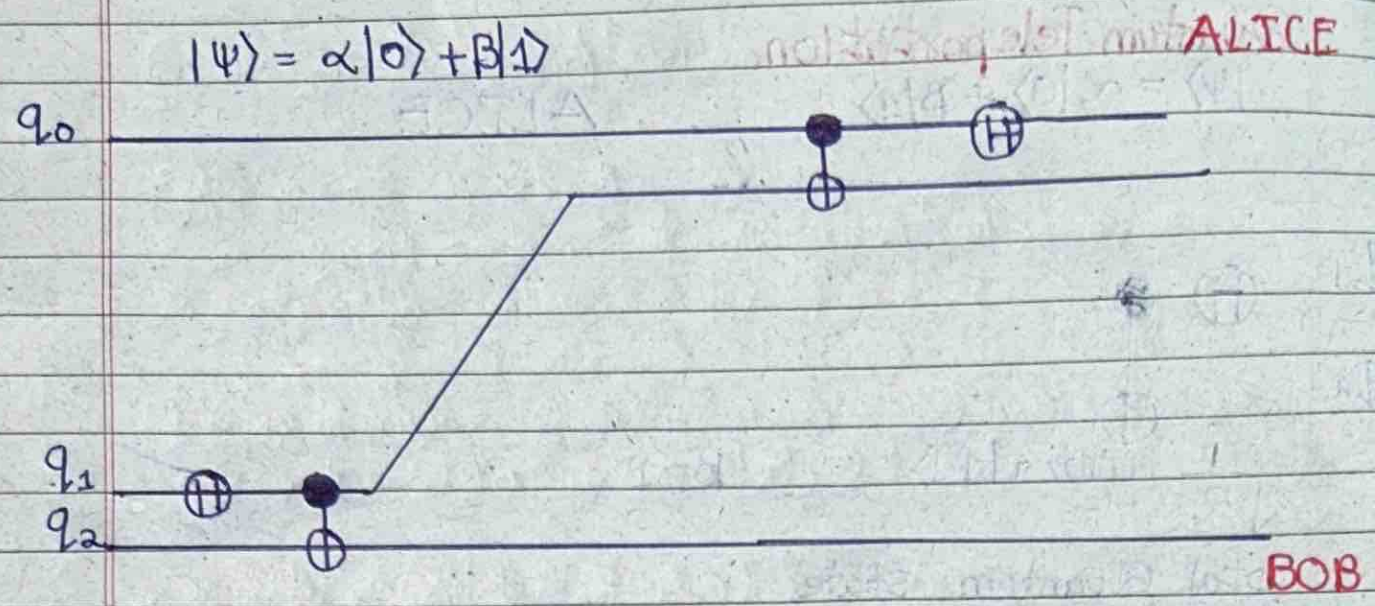


$\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$ BOB

$$\frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle]$$

$$\frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \beta|101\rangle + \beta|110\rangle]$$

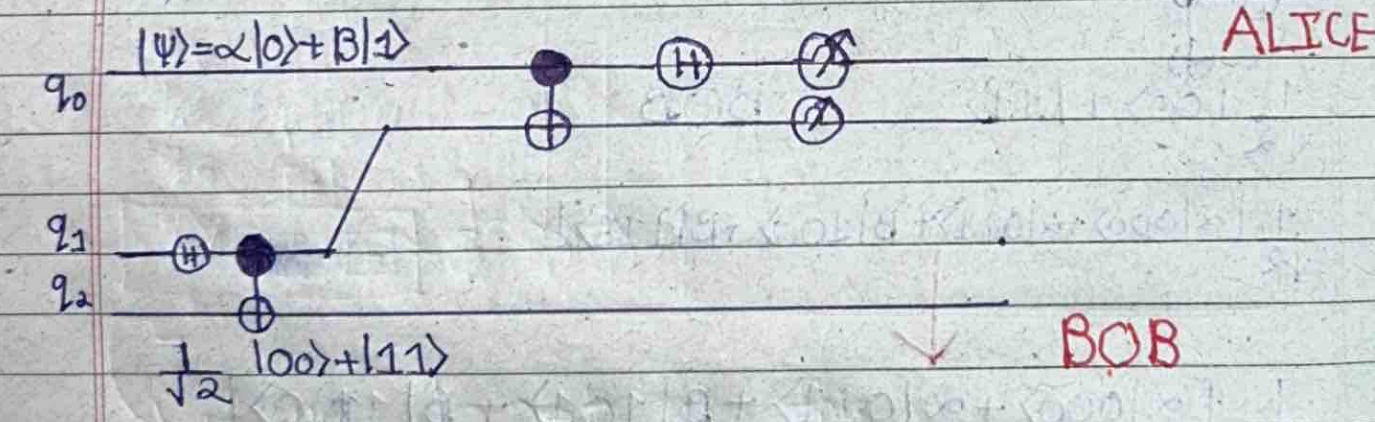
Only those problem !



Total Quantum State

$$\frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \beta|101\rangle + \beta|110\rangle]$$

$$\frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \alpha|100\rangle + \alpha|111\rangle + \beta|001\rangle + \beta|010\rangle - \beta|101\rangle - \beta|110\rangle]$$



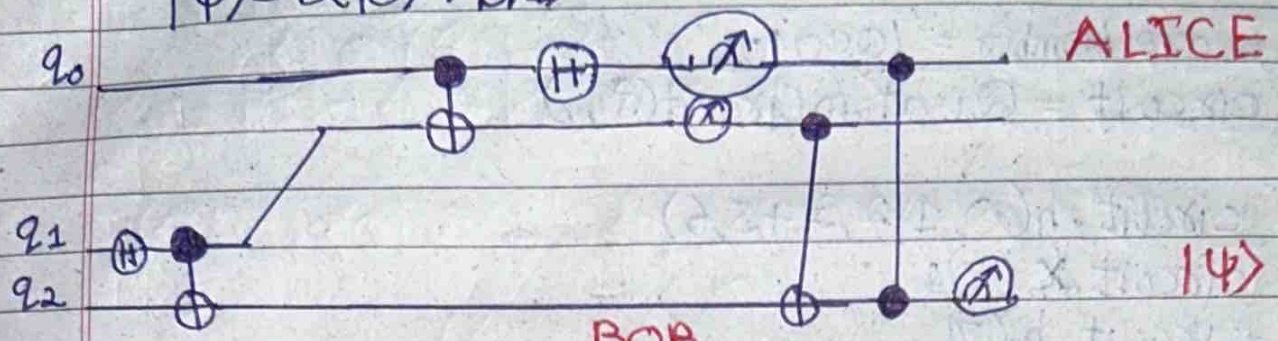
Measurement

$$\frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \alpha|100\rangle + \alpha|111\rangle + \beta|001\rangle + \beta|010\rangle - \beta|101\rangle - \beta|110\rangle]$$

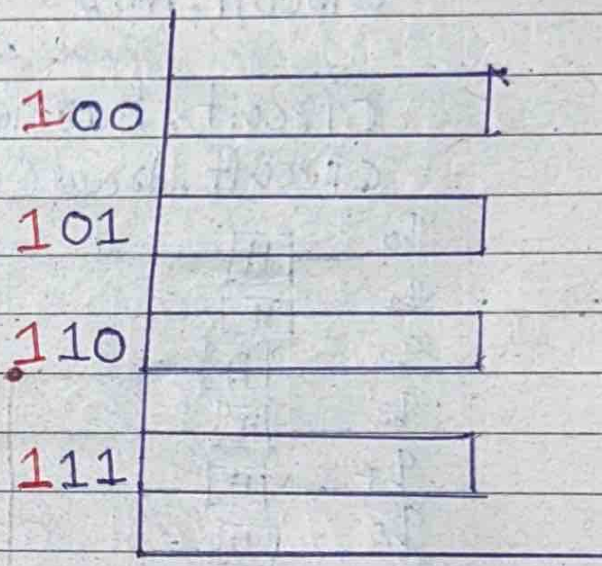
Q_0Q_1	00	01	10	11
Q_2	$\alpha\|0\rangle + \beta\|1\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$
	I	X	Z	XZ

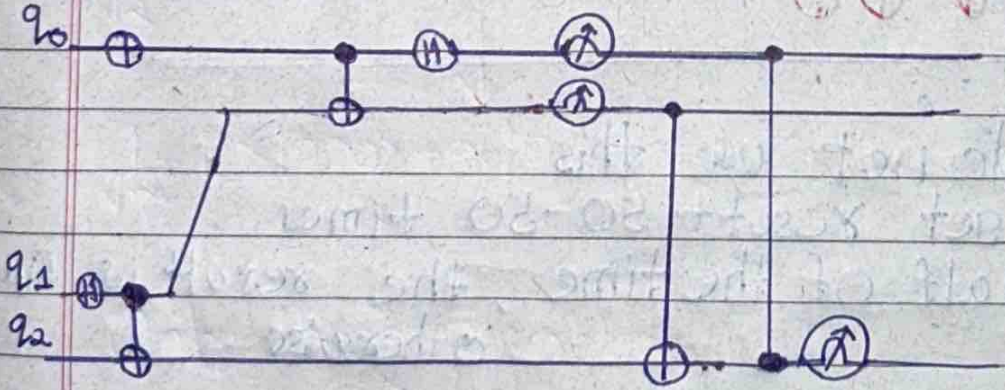
So, Now we need to do the same opperation as BOB
But will we use if statement ✗
control gate ✓

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



$\frac{1}{\sqrt{2}}|00\rangle + |11\rangle$



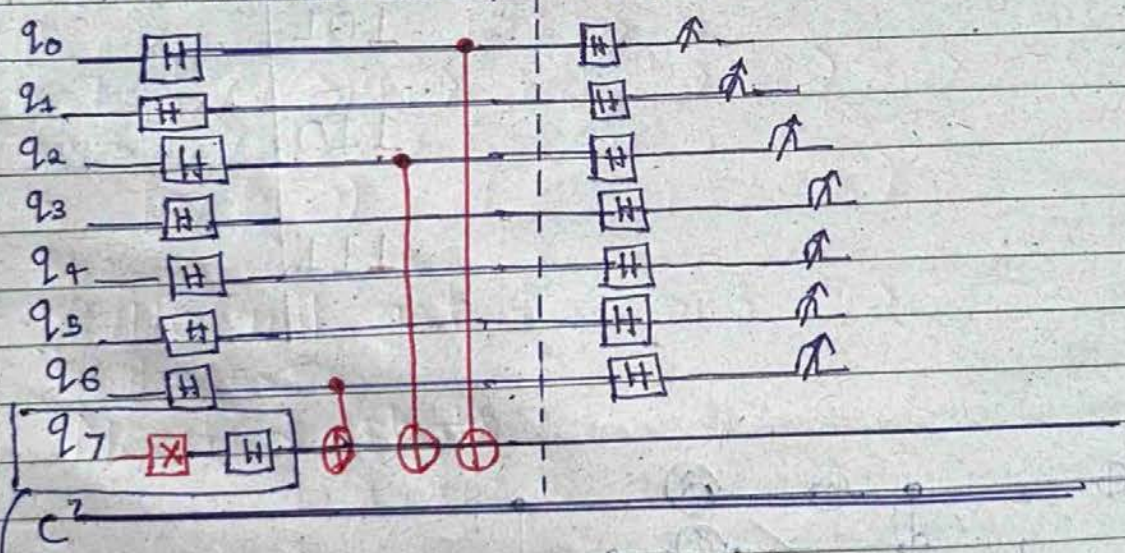


Only those problem that can be represented using quantum properties like
i) superposition ii) entanglement

Quantum Computer cannot perform Brute force

Bernstein Vazirani Algorithm

```
from qiskit import *
from qiskit.tools.tools.visualization import plot_histogram
%matplotlib inline

secreNumber = '1000101'
circuit = QuatumCircuit(8,7)

circuit.h(0,1,2,3,4,5,6)
circuit.x(7)
circuit.h(7)

circuit.barrier()
circuit.draw(output='mpl')
```



→ if we do not use this
We get result 50-50 times
Only half of the time, the result is fixed
otherwise

1 0 1 1 0 0 1

len = Brute force = ~~2^7 turns~~

turns = 2^7

And

```
  1 0 1 1 0 0 1
      AND
  0 0 0 0 0 0 1
```

[1]

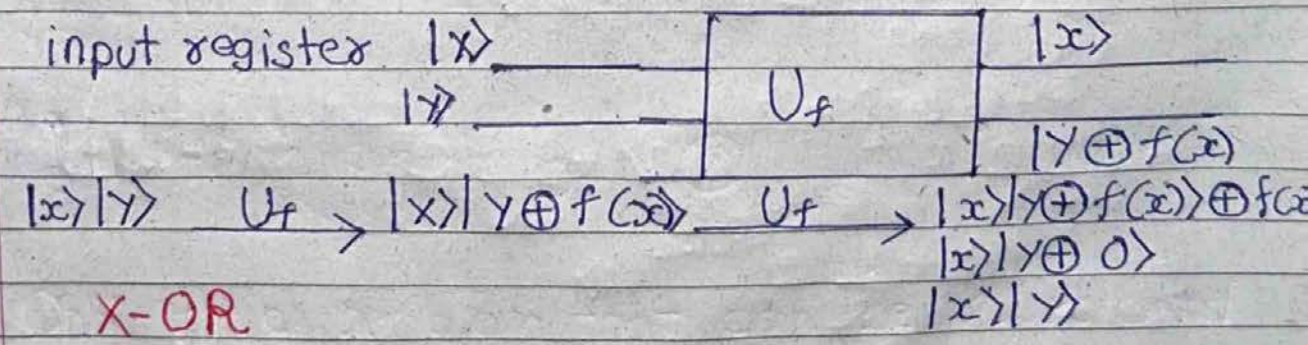
```
  1 0 1 1 0 0 1
      AND
  0 0 0 0 0 1 0
```

[1]

This way you will need 7 turn

Deutch Algorithm

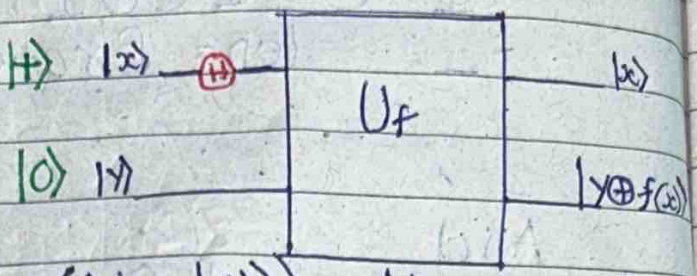
	f(0)	f(1)	input
1	0	0	constant
2	0	1	Balanced
3	1	0	Balanced
4	1	1	constant



X-OR

Deutsch Algorithm

Wrong approach



$$U_f(|+\rangle \otimes |0\rangle) \longrightarrow U_f\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right) \otimes |0\rangle$$

$$= \frac{1}{\sqrt{2}} U_f |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} U_f |1\rangle \otimes |0\rangle$$

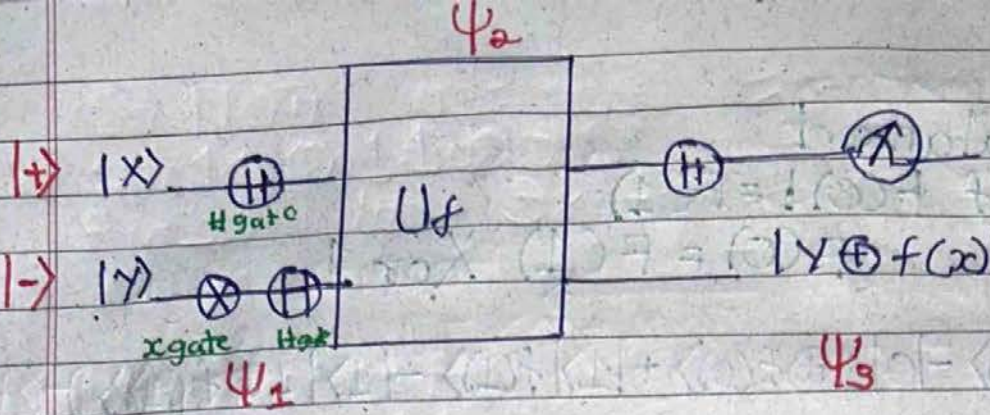
Now when you apply U_f first qubit will remain same

$$= \frac{1}{\sqrt{2}} U_f |0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}} U_f |1\rangle \otimes |0\rangle$$

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

$|0\rangle f(0)$ $|1\rangle f(1)$

// We will get this with 50% possibility
// Useless
Need 2 shots



$$\psi_1 = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

$$\rightarrow \frac{1}{2}(|0\rangle|0\oplus f(0)\rangle - |0|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1) - |1\oplus f(1)\rangle$$

$$\psi_2 = \frac{1}{2}(|0\rangle|f(0)\rangle - |0|\oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1\oplus f(1)\rangle$$

Now let us assume constant

$\therefore f(0) = f(1)$

$$= \frac{1}{2}(|0\rangle|f(0)\rangle - |0|1\oplus f(0)\rangle + |1\rangle|f0\rangle - |1\rangle|1\oplus f(0)\rangle$$

$$= \frac{1}{2}((|0\rangle + |1\rangle)|f(0)\rangle) + (-|0\rangle - |1\rangle)|1\oplus f(0)\rangle$$

$$= \frac{1}{2}$$

$$= \frac{1}{2}(|0\rangle + |1\rangle)(|f(0)\rangle - |1\oplus f(0)\rangle$$

$$= \frac{1}{2}|+\rangle(|f(0)\rangle - |1\oplus f(0)\rangle)$$

If we apply H gate on $|+\rangle$ we ge $|0\rangle$

$\psi_3 = H(|+\rangle) = |0\rangle$

; ignore the 2nd bit we are not even counting it

Not balanced

if $F(0) != F(1)$

$F(0) = F(1)$ X or 1

$$\psi_2 = \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)$$

$$= \frac{1}{2}(|0\rangle|f(0)\rangle - |0\rangle|f(1)\rangle + |1\rangle|f(1)\rangle - |1\rangle|f(0)\rangle)$$

$$= \frac{1}{2}(|0\rangle \otimes (|f(0)\rangle - |f(1)\rangle) - |1\rangle \otimes (|f(0)\rangle - |f(1)\rangle)$$

$$= \frac{1}{2}(|0\rangle - |1\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

$$= \frac{1}{2}(|-\rangle) \otimes (|f(0)\rangle - |f(1)\rangle)$$

Now apply H gate on $|-\rangle$ ignore the 2nd bit

ψ_3 $H(|-\rangle) = |1\rangle$

Shor's algorithm

1) Check if N is even or a prime power.
2) choose a random number (a)
   choose a random number a, where $1<a<N$
3) Calculate the GCD of (a, N)
   if GCD(a, N) > 1:
   Assumed NO is non trivial
4) Find the order (r) of a modulo N:
   The order r is the smallest +Ve integer such that $a^r \% N = 1$

Let us assume
N = 21 & a = 2

$2^1 \% 21 = 2$
$2^2 \% 21 = 4$
$2^3 \% 21 = 8$
$2^4 \% 21 = 16$
$2^5 \% 21 = 11$
$2^6 \% 21 = 1$
$2^7 \% 21 = 2$
$2^8 \% 21 = 4$

→ Pattern repeats after 6
r = 6

5) If r is even:
   continue
   If r is odd:
   select a different a [Go back to step 2]

6) Calculate the factors:
   $p = (a^{r/2} - 1, N) \rightarrow GCD$
   $q = GCD(a^{r/2} + 1, N)$

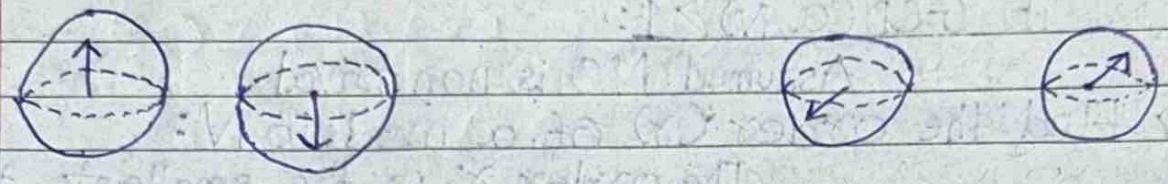
$= GCD(2^{6/2} - 1, 21) = GCD(2^3 - 1, 21) = GCD(7, 21) = 7$

$= GCD(2^{6/2} + 1, 21) = GCD(9, 21) = 3$

Shor's algorithm

Quantum Fourier Transform:

Computational Basis $\{|0\rangle, |1\rangle\}$ → Fourier Basis $\{|+\rangle, |-\rangle\}$



In Q.C, we do this opperation with help of the

$|QFT\rangle$

$$QFT|x\rangle = |\tilde{x}\rangle = \frac{1}{N} \sum_{y=0}^{N-1} e^{\frac{2*Pi.i.x.y}{N}} |y\rangle$$

Note, $e^{Pi.i} = -1$

$N = 2^n$

n = # Qubits

Let us substitute for : $N = 2^1$

$$= \frac{1}{\sqrt{2}} \sum_{y=0}^{2-1} e^{\frac{2.Pi.i.x.y}{2}} |y\rangle$$

$$= \frac{1}{\sqrt{2}} e^{\frac{2.Pi.i.x.0}{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{\frac{2.Pi.i.x.1}{2}} |1\rangle$$

$$= \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} e^{Pi.i*x} |1\rangle$$

Now, 2 possibilites

$x = 0$

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

$x = 1$

$$\frac{1}{\sqrt{2}} |0\rangle - |1\rangle \quad |-\rangle$$

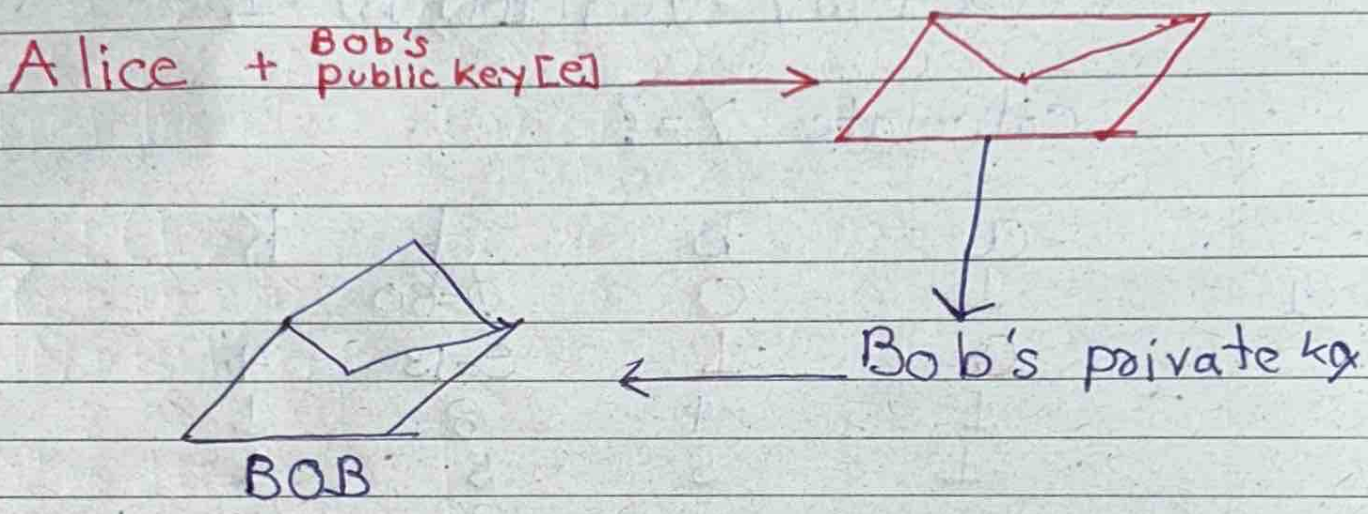
RSA

encryption

$$C = P^e \bmod n$$

decryption

$$P = C^d \bmod n$$



P ≡ plaintext
C ≡ ciphertext
p & q are prime number
e ≡ public key
ϕ ≡ Euler's phi Function
e ≡ Private key

Step 1

Let us assume

P = 7 and q = 11

$$\phi = (P-1)(q-1) = 60$$

Step 2: Select e,

conditions

i) $1 < e < \phi$

ii) e and ϕ should be co-prime

Step 3:

$d \times e \bmod \phi = 1$

$d \times 13 \bmod 60 = 1$

So,

$ax + by = gcd(a, b)$

$a = \phi$ and $b = e$

$60x + 13y = gcd(\$60, 13) = 1$

Calculate $Y = ?$

	a	b	d	K
1	1	0	$\phi = 60$	
	0	1	$e = 13$	4
	1	-4	8	1
	-1	5	5	1
	2	-9	3	1
	-3	14	2	1
	5	[-23]	1	

Step IV

set d

```
if (b > ϕ)
  {
    d = b % ϕ
  }
if (b is -ve)
  {
    d = b + ϕ
  }
```

$d = -23 + 60 = 37$

Let us check

$P = 7$ [asumed]
$q = 11$
$\phi = 60$ [calculated]
$n = P * q = 77$ [calculated]
$e = 13$ [Assumed according to conditio]
$d = 37$ [Calculated]

Encryption

$C = P^e \bmod n$
$= 40^{13} \% 77$
$= 68$

Decryption

$P = C^d \bmod n$
$= 68^{37} \% 77$
$= 40$