Fundamentals of Quantum computing

what is quantum computing?

⇒ When computation is done using the principles of quantum mechanics, it is called quantum computing.

Review of Linear Algebra

→ A Hilbert space H is a normed vector space over the complex numbers C.

→ Dirac's bra-ket Notation

z^* - complex conjugate, if $z = a+ib$, then $z^* = a-ib$.

The "ket" $|\psi\rangle$ corresponds to a column vector ψ. ψ^+ is conjugate transpose of a vector ψ.

$$\begin{bmatrix} \text{bra-ket} \\ \langle \quad \rangle \end{bmatrix} \quad \begin{matrix} |\psi\rangle : \text{ket} \\ \langle\psi| : \text{bra} \end{matrix}$$

Example:-

$$\psi = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \qquad \psi^+ = (\bar{a}_1 \dots \bar{a}_n)$$

In Dirac's notation, the conjugate transpose of a ket $|\psi\rangle$ is called a "bra" & is written as $\langle\psi|$. Hence,

$$|\psi\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \quad \& \quad \langle\psi| = (\bar{a}_1 \dots \bar{a}_n)$$

A bra $\langle\psi|$ corresponds to a row vector ψ^+.

Inner Product between vector $|\psi\rangle$ & $|\phi\rangle$

$$|\psi\rangle = \begin{bmatrix} \psi_1 \\ \vdots \\ \psi_n \end{bmatrix} \quad \& \quad |\phi\rangle = \begin{bmatrix} \phi_1 \\ \vdots \\ \phi_n \end{bmatrix}$$

The inner product $\langle\psi|\phi\rangle$ is defined to be the scalar obtained by multiplying the conjugate transpose $\langle\psi| = (\bar{\psi}, \dots \bar{\psi_n})$ with $|\phi\rangle$.

$$\langle \psi | \phi \rangle = (\bar{\psi}_1, \dots \bar{\psi}_n) \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix} = \sum_{i=1}^{n} \bar{\psi}_i \phi_i$$

$i = \sqrt{-1}$
$i^2 = -1$

Example:

$$|\psi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix} \quad |\phi\rangle = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$\langle \psi | \phi \rangle = \begin{bmatrix} 2 & -6i \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix}$$

$$= 6 - 24i$$

Tensor product of $|\psi\rangle$ & $|\phi\rangle$

It is given by

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle$$

Example:

$$|\psi\rangle|\phi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix} \otimes \begin{bmatrix} 3 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \times 3 \\ 2 \times 4 \\ 6i \times 3 \\ 6i \times 4 \end{bmatrix} = \begin{bmatrix} 6 \\ 8 \\ 18i \\ 24i \end{bmatrix}$$

ψ^+ - Hermition conjugate (adjoint) of matrix ψ.

if $\psi = \begin{bmatrix} 1 & 6i \\ 3i & 2+4i \end{bmatrix}$ then $\psi^+ = \begin{bmatrix} 1 & -3i \\ -6i & 2-4i \end{bmatrix}$. Note $\psi^+ = (\bar{\psi})^t$

$\||\psi\rangle\|$ - norm of vector $|\psi\rangle$

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

Normalization of $|\psi\rangle$ is given by $\dfrac{|\psi\rangle}{\||\psi\rangle\|}$

Ex: Find norm $|\psi\rangle = \begin{bmatrix} 1 \\ 2 \\ -i \end{bmatrix}$

$$\||\psi\rangle| = \sqrt{\langle \psi | \psi \rangle} = ? \quad \sqrt{6}$$

$\langle\psi|\psi\rangle = (1 \;\; 2 \;\; i)\begin{pmatrix}1\\2\\-i\end{pmatrix} = 1+4+1 = 6$

Normalization of $|\psi\rangle = \dfrac{|\psi\rangle}{\||\psi\rangle\|} = \dfrac{1}{\sqrt{6}}\begin{pmatrix}1\\2\\-i\end{pmatrix}$

$\left(\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, \frac{i}{\sqrt{6}}\right)\begin{pmatrix}\frac{1}{\sqrt{6}}\\ \frac{2}{\sqrt{6}}\\ \frac{-i}{\sqrt{6}}\end{pmatrix} = \frac{1}{6}+\frac{4}{6}+\frac{1}{6} = \frac{6}{6} = 1$

$= \||\phi\rangle\| = \sqrt{\langle\phi|\psi\rangle}$

Unit vector:
A normalized vector or unit vector $|\psi\rangle$ is a vector whose norm is 1.

Orthogonal vectors:
Two vectors $|\psi\rangle$ and $|\phi\rangle$ is said to be orthogonal if their inner product is zero.

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

Ex: $|\psi\rangle = \begin{pmatrix}i\\i\end{pmatrix}$ $|\phi\rangle = \begin{pmatrix}1\\-1\end{pmatrix}$

$\langle\psi|\phi\rangle = (-i \;\; -i)\begin{pmatrix}1\\-1\end{pmatrix}$

$= -i+i = 0$

Problems- If $|x\rangle = \begin{pmatrix}1\\i\\2+i\end{pmatrix}$ $|y\rangle = \begin{pmatrix}2-i\\1\\2+i\end{pmatrix}$

Find $\||x\rangle\|$, $\langle x|y\rangle$, $\langle y|x\rangle$

Prove that $\langle x|y\rangle = \langle y|x\rangle^*$

$\||x\rangle\| = \sqrt{\langle x|x\rangle} = \sqrt{7}$

$\langle x|x\rangle = (1, -i, 2-i)\begin{pmatrix}1\\i\\2+i\end{pmatrix}$

$= 1+1+5 = 7$

$$\langle x|y| = (1-i, 2-i)\begin{pmatrix} 2-i \\ 1 \\ 2+i \end{pmatrix}$$

$$= \underline{7-2i}$$

$$\langle y|x\rangle = (2+i, 1, 2-i)\begin{pmatrix} 1 \\ i \\ 2+i \end{pmatrix} = \underline{7+2i}$$

$$\boxed{7-2i = (7+2i)^* = 7-2i}$$ Hence proved.

Linearly Independent vectors-

The set of vectors $|\psi_1\rangle, \ldots |\psi_n\rangle$ in $\mathbb{C}^n$ are said to be linearly independent if there exists scalars $a_1 \ldots a_n$ such that

$$a_1|\psi_1\rangle + a_2|\psi_2\rangle + \ldots + a_n|\psi_n\rangle = 0$$

$$\Rightarrow a_1 = a_2 = \ldots = a_n = 0$$

Ex: The vector $|\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ & $|\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ linearly independent

$$a_1|\psi_1\rangle + a_2|\psi_2\rangle = 0$$

$$a_1\begin{pmatrix} 1 \\ 0 \end{pmatrix} + a_2\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

$$a_1 + a_2 = 0$$

$$\Rightarrow a_1 = 0, \; a_2 = 0$$

Linearly dependent vectors-

The set of vectors $|\psi_1\rangle, \ldots |\psi_n\rangle$ in $\mathbb{C}^n$ are said to be linearly dependent if there exists scalars $a_1 \ldots a_n$, not all of them are 0, such that-

$$a_1|\psi_1\rangle + a_2|\psi_2\rangle + \ldots + a_n|\psi_n\rangle = 0$$

Ex: The vectors $|\psi_1\rangle = \begin{pmatrix} 1 \\ 2 \\ -9 \end{pmatrix}$ & $|\psi\rangle = \begin{pmatrix} -2 \\ -4 \\ 18 \end{pmatrix}$

are linearly dependent in $\mathbb{C}^3$.

$$a_1|\psi_1\rangle + a_2|\psi_2\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$a_1\begin{pmatrix} 1 \\ 2 \\ -9 \end{pmatrix} + a_2\begin{pmatrix} -2 \\ -4 \\ 18 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$\Rightarrow a_1 = 2 \quad a_2 = 1$

Ex: The vectors $|\psi_1\rangle = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $|\psi_2\rangle = \begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix}$

$|\psi_2\rangle = \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix}$ are linearly independent.

$$a_1|\psi_1\rangle + a_2|\psi_2\rangle + a_3|\psi_3\rangle = 0$$

$$a_1\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + a_2\begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix} + a_3\begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} a_1 + 2a_2 + a_3 \\ 2a_1 + 5a_2 + 3a_3 \\ 3a_1 + 7a_2 + 5a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$\Rightarrow a_1 + 2a_2 + a_3 = 0$

$2a_1 + 5a_2 + 3a_3 = 0$

$3a_1 + 7a_2 + 5a_3 = 0$

$\Rightarrow a_1 = a_2 = a_3 = 0$

Basis - The set of vectors $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ is said to be basis for $\mathbb{C}^n$, then every vector $|v\rangle$ can be uniquely expressed as a linear combination of $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$ i.e. $|v\rangle = a_1|\psi_1\rangle + a_2|\psi_2\rangle + \cdots + a_n|\psi_n\rangle$

where $a_1, \ldots, a_n$ are scalars.

Ex: The vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is basis in $\mathbb{C}^2$.

$|v\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \qquad \begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Note - A basis for C^n consists of exactly n linearly independent vectors.

Orthonormal basis -

A basis is said to be orthonormal if each vector has norm 1 and each pair of vectors are orthogonal.

Ex- The vectors $|\psi_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|\psi_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are orthonormal basis in C^2.

$$\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle} = \sqrt{1} = 1$$

orthogonal → inner product is zero.

$$\langle \psi_1 | \psi_1 \rangle = (1 \;\; 0) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$

$$\| |\psi_2\rangle \| = \sqrt{\langle \psi_2 | \psi_2 \rangle} = \sqrt{1} = 1$$

$$\langle \psi_1 | \psi_2 \rangle = (0 \;\; 0) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0$$

Ex: 1. The vectors $|\phi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ & $|\phi_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$

are orthonormal basis in C^2.

2. The vectors $|v_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$ $|v_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$ are orthonormal basis in C^2.

$$\langle v_1 | v_2 \rangle = \left(\frac{1}{\sqrt{2}} \;\; -\frac{1}{\sqrt{2}} \right) \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} - \frac{1}{2} = 0$$

$$\| |v_1\rangle | = \sqrt{\langle v_1 | v_1 \rangle}$$

$$\langle v_1 | v_1 \rangle = \left(\frac{1}{\sqrt{2}} , \frac{-i}{\sqrt{2}} \right) \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} + \frac{1}{2} = 1$$

Postulates of Quantum Mechanics

Postulate 1: Definition of quantum bit or qubit

Postulate 2: How qubit(s) transform (evolve)

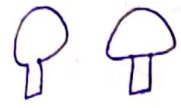
Postulate 3: The effect of measurement.

Postulate 4: How qubits combine together into systems of qubits.

c bit

0 or 1

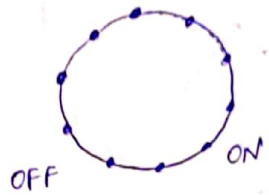
light



0 1

qubit

$|0\rangle$ or $|1\rangle$



$|\psi\rangle = \alpha\,\text{OFF} + \beta\,\text{ON}$

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

qubit: In quantum mechanics two possible states for a qubit are $|0\rangle$ and $|1\rangle$.

These qubits can be expressed as orthonormal basis vectors in $\mathbb{C}^2$.

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

A generic qubit state $|\psi\rangle$ in represented by linear combination (or superposition) of $|0\rangle$ and $|1\rangle$.

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

where α and β are complex members with

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

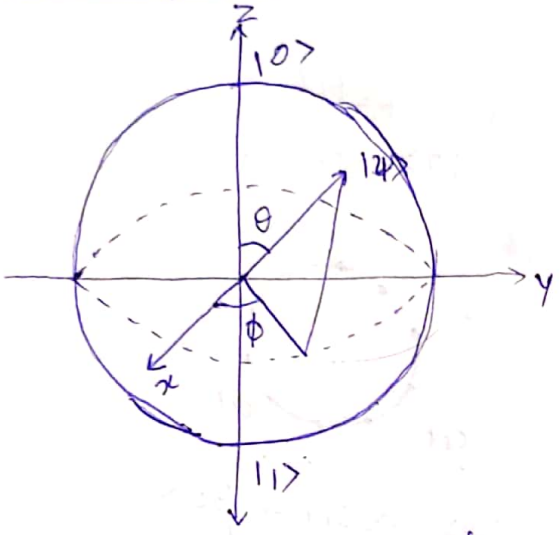
When we measure qubit we get 0 with probability $|\alpha|^2$ or ~~weight~~ we get 1 with probability $|\beta|^2$.

Example-

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

After measurement we get 0 with probability $\frac{1}{2}$ or we get 1 with probability $\frac{1}{2}$.

Bloch sphere



Block sphere or unit sphere

$$x^2 + y^2 + z^2 = 1$$

The state $|\psi\rangle$ of a qubit is represented by a point on the surface of a sphere of unit radius, called Bloch sphere.

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

$$\alpha = \cos\frac{\theta}{2}$$

$$\beta = e^{i\phi}\sin\frac{\theta}{2} \qquad |\alpha|^2 + |\beta|^2 = 1$$

Multiple qubits

2-qubit system has 4 possible states—

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

A generic qubit state describing the 2-qubits is given by—

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = (1\ 0\ 0\ 0)^T$$

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

$$= (0\ 1\ 0\ 0)^T$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = (0\ 0\ 1\ 0)^T$$

$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = (0\ 0\ 0\ 1)^T$

$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$

$= \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$

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

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

Entangled States:

States that cannot be written as the tensor product of n single qubit states are entangled states.

Ex- Consider the state –

$\gamma_1|00\rangle + \gamma_2|11\rangle$, with $\gamma_1 \neq 0$ and $\gamma_2 \neq 0$

This can not be written as

$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$

The entangled states known as Bell states or EPR pairs (Einstein, Podolsky, Rosen)

Examples: The following two-qubit states are –

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

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

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

$|\psi-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ are entangled.

* P.T. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ in an entangled state.

It is impossible to find $\alpha_1 \beta_1 \alpha_2 \beta_2$ such that

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

Since we have,

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

If $\alpha_1\beta_2 = 0$ implies $\alpha_1\alpha_2 = 0$ or $\beta_1\beta_2 = 0$ this is impossible.

2) P.T $\frac{1}{\sqrt{2}}(|00> + |01>)$ is not entangled state.

$\rightarrow |00> = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01> = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$

$\frac{1}{\sqrt{2}}(|00> + |01>) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \\ 0 \\ 0 \end{bmatrix}$

$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right] = |0> \otimes \frac{1}{\sqrt{2}}(|0> + |1>)$

Since it can be written as single qubit state it is not entangled.

3) PT $\frac{1}{\sqrt{2}}(|00> - |01>)$ is not entangled state.

$|00> = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01> = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$

$\frac{1}{\sqrt{2}}(|00> - |01>) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \\ 0 \\ 0 \end{bmatrix}$

$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

$= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \times \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$

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

Problems:

1. Show the following 2-qubit states are entangled

a) $\frac{1}{\sqrt{2}}(|00\rangle - i|11\rangle)$ b) $\frac{i}{10}|00\rangle + \frac{\sqrt{99}}{10}|11\rangle$

3-qubit entangled state (GHz state)

The state $|GHz\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ is 3-qubit entangled state.

It is called Greenberger-Horne-Zeilinger (GHZ) state.

Face-flip gate

$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

Hermitian Matrix:

A complex matrix A is said to be Hermition of $A^+ = A$ $(A^+ = (\bar{A})^T$ = conjugate transpose of A).

Unitary matrix

A complex matrix A is said to be unitary if $A^+A = I$ or $A^+ = A^{-1}$.

Eigen value and Eigen vectors:

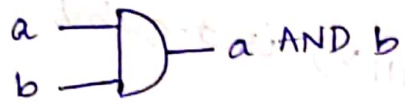
Let A be any complex square matrix. A scalar λ is called an eigen value of A if there exists a non-zero column vector $|v\rangle \in \mathbb{C}^n$ such that $A|v\rangle = \lambda|v\rangle$, $\lambda \in C$.

The vector $|v\rangle$ is called an eigen vector of A corresponding to λ.

Quantum computation

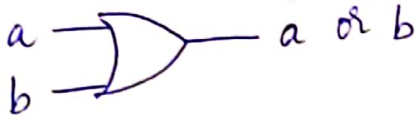
A quantum computer is built from quantum circuit containing wires and elementary quantum gates to carry around and manipulate quantum information

AND gate



NAND gate

OR gate



NOR gate

NOT gate

Single qubit Quantum gate

1. Quantum NOT gate (X gate or bit flip gate) we define a matrix X to represent the quantum NOT gate by —

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

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

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

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

$$= \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

$\alpha|0\rangle + \beta|1\rangle$ — [X] — $\beta|0\rangle + \alpha|1\rangle$

X is unitary $X^t X = I$

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

Single qubit Quantum gate

Z gate (phase flip gate).

Z gate is defined by the matrix, $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

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

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

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

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{Z}} \alpha|0\rangle - \beta|1\rangle$$

Hadamard gate (H-gate):

H-gate is defined by the matrix —

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

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

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

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

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

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{H}} \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{\beta|0\rangle - |1\rangle}{\sqrt{2}}$$

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

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

X-gate

$|0\rangle \to |1\rangle$

$|1\rangle \to |0\rangle$

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

$X^+ X = I$

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

Z-gate

$|0\rangle \to |0\rangle$

$|1\rangle \to -|1\rangle$

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

$Z^+ Z = I$

H-gate

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

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

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

$H^+ H = I$

Y-gate

$|0\rangle \to -i|1\rangle$

$|1\rangle \to -(-i)|0\rangle$

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

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

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

$\alpha|0\rangle + \beta|1\rangle$ — [Y] — $i(\alpha|1\rangle - \beta|0\rangle)$

$Y^+ Y = I$

Phas-shift gate

$|0\rangle \to |0\rangle$

$|1\rangle \to e^{i\theta}|1\rangle$

$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ θ is any value.

$R_\theta|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

$R_\theta|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ e^{i\theta} \end{bmatrix} = e^{i\theta}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = e^{i\theta}|1\rangle$

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

when $\theta = \pi$, } so we get a z gate.

$e^{i\pi} = -1$

Problems

1. write the following quantum gates in bra/ket notation.

i) X, ii) Z iii) H iv) Y v) R_θ

i) $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

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

$= |1\rangle\langle 0| + |0\rangle\langle 1|$

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

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

$|00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle$

$|00\rangle = |0\rangle \otimes |0\rangle$

$= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

~~to~~ $|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$

Two-qubit controlled gate

→ Controlled NOT gate: It flips the second bit if the first bit is 1 and does nothing otherwise.

C_{NOT} : $|00\rangle \rightarrow |00\rangle$

$|01\rangle \rightarrow |01\rangle$

$|10\rangle \rightarrow |11\rangle$

$|11\rangle \rightarrow |10\rangle$

The matrix form of this is—

$$C_{NOT}: \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

C_{NOT} is unitary.

$C_{NOT}\ C_{NOT}^{+} = I$

C_{NOT} is a generalization of the classical XOR gate because $|AB\rangle \longrightarrow |AB \oplus A\rangle$

The C_{NOT} gate cannot be decomposed into a tensor product of 2 single qubit states.

- C_{NOT} takes the entangles qubit state.

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \oplus |0\rangle$ to the entangled state.

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

$$C_{NOT}\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}\right) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right] = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Qubits are not copy bits.

The NO-cloning principle

→ The no cloning principle states that we cannot copy or clone an unknown qubit.

→ Let U is a unitary transformation that clones i.e. $U(|00\rangle) = |aa\rangle$, for all quantum states $|a\rangle$.

→ Let $|a\rangle$ & $|b\rangle$ be 2 orthonormal quantum states consider $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$

$U(|c0\rangle = U\left(\frac{1}{\sqrt{2}}(|a0\rangle + |b0\rangle)\right)$

$= \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)$

But $U(|c0\rangle) = |cc\rangle = |c\rangle \otimes |c\rangle$

$= \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle)$

$\neq \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)$

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

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

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

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

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

C_{NOT} $|A\rangle$ — $|A\rangle$

$|B\rangle$ — ⊕ — $|B \oplus A\rangle$

SWAP gate

simply exchanges bit values.

$|00\rangle \longrightarrow |00\rangle$

$|01\rangle \longrightarrow |10\rangle$

$|10\rangle \longrightarrow |01\rangle$

$|11\rangle \longrightarrow |11\rangle$

In matrix form —

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

Tensor product for matrices

Consider 2 vectors

$$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \quad |w\rangle = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$

$$|v\rangle \otimes |w\rangle = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \otimes \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$$

$$= \begin{bmatrix} v_1 \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \\ v_2 \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \end{bmatrix} = \begin{pmatrix} v_1 w_1 \\ v_2 w_2 \\ v_2 w_1 \\ v_2 w_2 \end{pmatrix}$$

Suppose we have 2 matrices -

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}_{2\times 2} \qquad N = \begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix}_{2\times 2}$$

The tensor product of M & N is defined as -

$$M \otimes N = \begin{bmatrix} m_1 \cdot \begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix} & m_2 \cdot \begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix} \\ m_3 \cdot \begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix} & m_4 \cdot \begin{bmatrix} n_1 & n_2 \\ n_3 & n_4 \end{bmatrix} \end{bmatrix}$$

$$= \begin{bmatrix} m_1 n_1 & m_1 n_2 & m_2 n_1 & m_2 n_2 \\ m_1 n_3 & m_1 n_4 & m_2 n_3 & m_2 n_4 \\ m_3 n_1 & m_3 n_2 & m_4 n_1 & m_4 n_2 \\ m_3 n_3 & m_3 n_4 & m_4 n_3 & m_4 n_4 \end{bmatrix}_{4\times 4}$$

1. Find tensor product of X-gate and Z-gate.

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

Quantum Measurement :-

Quantum State-

The collection of all relevant physical properties of quantum system (for example, position, momentum, spin, polarization) is known as the state of the system.

Physical support	Name	Info. support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization	Polarization	Vertical	Horizontal
Electron	Electronic spin	spin	up ↑	down ↓

For example, if we use the energy of an electron as our qubits $|0\rangle$ & $|1\rangle$, we could say that the ground state (lowest energy) is our qubit $|0\rangle$ & an excited state (higher energy) is our qubit $|1\rangle$.

Ground state $= |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

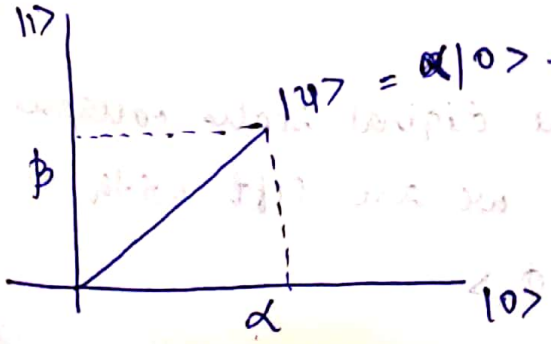
Excited state $= |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

We can define state $|+\rangle$ and $|-\rangle$ with the vectors.

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

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

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

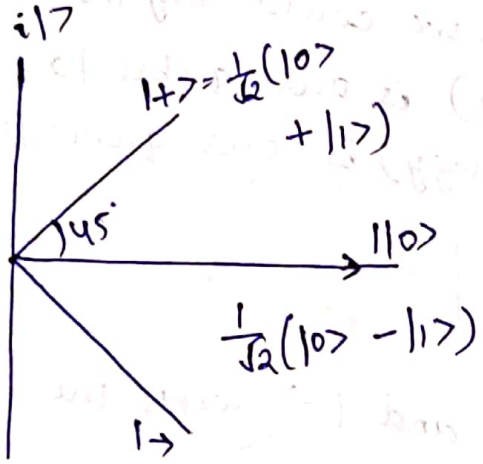


|0⟩ off
|1⟩ on
|ψ⟩ = α off + β on

- Quantum mechanics describes the behavior of s/m such as electrons, photons or molecules. we use mathematics to model these physical phenomena.
- Consider general quantum state.
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α, β & $|\alpha|^2 + |\beta|^2 = 1$
- When we measure quantum state $|\psi\rangle$ we get either the result $|0\rangle$ with probability $|\alpha|^2$ or we get result $|1\rangle$ with prob. $|\beta|^2$.

$\{|0\rangle, |1\rangle\}$ $\{|+\rangle, |-\rangle\}$

$\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}$ $\left\{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\right\}$



Defn: Born's rule: Suppose we have a quantum state $|\psi\rangle$ and orthonormal basis $\{|\phi_1\rangle, \ldots, |\phi_n\rangle\}$. Then we measure $|\psi\rangle$ wrt this orthonormal basis i.e. we ask the quantum s/m which one of these states its in.
- The probability of measuring states $|\phi_i\rangle$ is given by

$$P(\phi_i) = |\langle\phi_i|\psi\rangle|^2$$

- After the measurement the original states collapses in the measured state i.e. we are left with one of the states $|\phi_1\rangle \ldots |\phi_n\rangle$

Ex: Given a quantum state

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

we measure $|\psi\rangle$ in std computational basis.

$\{|0\rangle, |1\rangle\}$ the outcome states will be

$|0\rangle$ with prob $|\langle 0|\psi\rangle|^2 = |\alpha|^2$

$|1\rangle$ with prob $|\langle 1|\psi\rangle|^2 = |\beta|^2$

$|\langle 0|\psi\rangle|^2 = |(1,0)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}|^2 = |\alpha|^2$

$|\langle 1|\psi\rangle|^2 = |(0,1)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}|^2 = |\beta|^2$

Ex: what will be the outcome if we measure in $\{|+\rangle, |-\rangle\}$

$|+\rangle$, with prob $|\langle +|\psi\rangle|^2 = \frac{(\alpha+\beta)^2}{2}$

$|-\rangle$ with prob $|\langle -|\psi\rangle|^2 = \frac{(\alpha-\beta)^2}{2}$

- Given a quantum state $|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ i\end{pmatrix}$ what is the probability of measuring it in the state $|+\rangle$.

$P(+) = |\langle +|\psi\rangle|^2$ $\qquad |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}$

$= \left|\frac{1}{2}(1,1)\begin{pmatrix}1\\ i\end{pmatrix}\right|^2$

$= \frac{1}{4}|1+i|^2 = \frac{1}{4}\left((1+i)(1-i)\right) = \frac{2}{4} = \frac{1}{2}$

$[\,|z|^2 = z\bar{z}\,]$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$

$|0\rangle$ $|\alpha|^2$

$|1\rangle$ $|\beta|^2$

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

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

$-\frac{9}{5} + \frac{1}{5} = -\frac{8}{5} \neq 1$

$\therefore$ Not valid

$|v\rangle = \frac{|v\rangle}{\||v\rangle\|}$

$z = a + ib$

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

$|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$

$|0\rangle \quad 1/5$

$|1\rangle \quad 4/5$

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

$\therefore$ Thus its valid.

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

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

$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

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

$|0\rangle \quad 1/9$

$|1\rangle \quad 8/9$

Measuring 2-qubits

The general state of 2-qubit system is written as-

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

where $\alpha_1, \beta_1, \alpha_2, \beta_2 \in C$ and

$|\alpha_1|^2 + |\beta_1|^2 + |\alpha_2|^2 + |\beta_2|^2 = 1$

Then we have the following measurement rules-

$|00\rangle$: with probability $|\alpha_1|^2$

$|01\rangle$: " — " — $|\beta_1|^2$

$|10\rangle$: " — " — $|\alpha_2|^2$

$|11\rangle$: " — " — $|\beta_2|^2$

But we don't have to measure both qubits at once. Let us say we measure only the first qubit and get result $|0\rangle$.

- The only way we could get this is from the terms in $|00\rangle$ and $|01\rangle$.

$\{|0\rangle$: with probability $|\alpha_1|^2 + |\beta_1|^2$

The new state is -

$$|\psi'\rangle = \frac{\alpha_1 |00\rangle + \beta_1 |01\rangle}{\sqrt{|\alpha_1|^2 + |\beta_1|^2}}$$

We now measure the second qubit. From the coeffecients in the new state, we must have

$$\begin{cases} |0\rangle \text{ with probability } \dfrac{|\alpha_1|^2}{|\alpha_1|^2 + |\beta_1|^2} \\ |1\rangle \text{ " —— " —— - } \dfrac{|\beta_1|^2}{|\alpha_1|^2 + |\beta_1|^2} \end{cases}$$

The new state will be either $|00\rangle$ or $|01\rangle$ depending on whether the result was $|0\rangle$ or $|1\rangle$.

Measuring multi-qubit state

i) Consider 2-qubit state

$$|\psi\rangle = \frac{1}{3}|00\rangle + \frac{2}{3}|10\rangle - \frac{2}{3}|11\rangle$$

a) what is the probability that the result is $|0\rangle$?

b) what is the probability that the result is $|1\rangle$.

c) For each possible result, write down post-measurement state.

d) Calculate the probability that a measurement of the 2nd qubit will give 0 and 1. Write down the states after the 2nd measurement.

a) $\frac{1}{9}$, $|\psi'\rangle = |00\rangle$

Subsequent measurement of 2nd qubit gives $|0\rangle$ with probability 1. or $|1\rangle$ with probability 0.

post-measurement state is $|00\rangle$.

b) $\frac{8}{9}$, $|\psi'\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle)$

Subsequent measurement of 2nd qubit gives $|0\rangle$ with probability $\frac{1}{2}$ or $|1\rangle$ with probability $\frac{1}{2}$. with post-measurement state $|10\rangle$ or $|11\rangle$.

1. Consider the 2-qubit quantum state.

$$|\psi\rangle = \frac{1}{2}|00\rangle - \frac{1}{\sqrt{3}}|10\rangle + \frac{1}{2}|01\rangle + \frac{i}{\sqrt{6}}|11\rangle$$

a) what is the probability the result $|0\rangle$.

$\frac{1}{2}$.

Post measurement state.

$$|\psi'\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle$$

A subsequent measurement of the second bit gives $|0\rangle$ with probability $\frac{1}{2}$ or $|1\rangle$ with probability $\frac{1}{2}$. Then post-measurement states are $|00\rangle$ and $|01\rangle$ respectively.

b) what is the probability the result is $|1\rangle$?

$\frac{1}{2}$

Post measurement state

$$|\psi'\rangle = -\sqrt{\frac{2}{3}}|10\rangle + i\frac{1}{\sqrt{3}}|11\rangle$$

A subsequent measurement of second bit gives $|10\rangle$ with probability $\frac{2}{3}$ and $|11\rangle$ with probability $\frac{1}{3}$.

Quantum circuits :

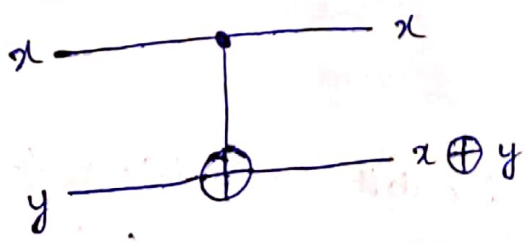
Reversible computation -

A boolean gate G is said to be reversible if it has the same number of inputs as outputs and its mapping from input strings to output strings is a bijection.

$(x,y) \rightarrow (y,x)$

CNOT is reversible

CNOT diagram :



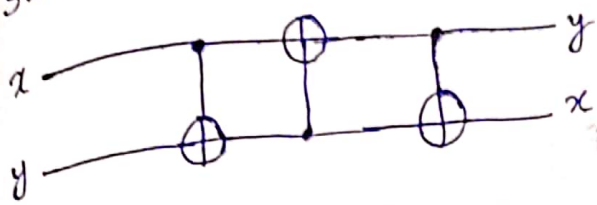
copy operation using CNOT:

CNOT performs the copy operation if y is initially set to zero.

CNOT : $(x,0) \rightarrow (x,x)$

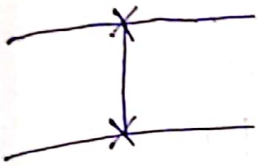
SWAP operation using CNOT:

SWAP with 3 CNOT gate.

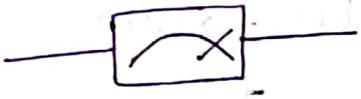


$(x,y) \rightarrow (x, x \oplus y) \rightarrow (y, x \oplus y) \rightarrow (y,x)$.

ICON for SWAP gate



The diagram for measurement is —



Basic examples of quantum circuits-

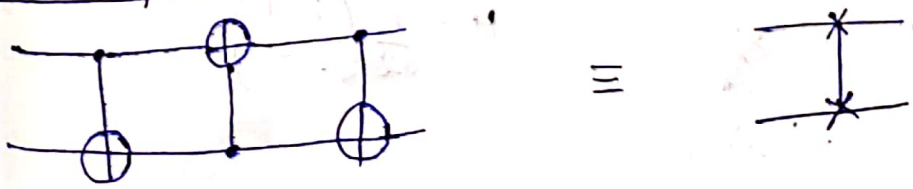
1) $|0\rangle$ — H — $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$

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

3) $|0\rangle$ — X — $|1\rangle$

4) $|1\rangle$ — X — $|0\rangle$

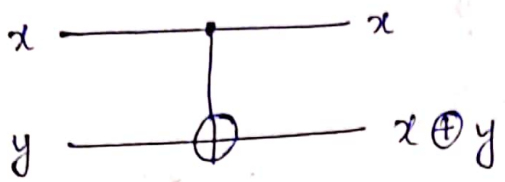
SWAP - operation



CNOT operation

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

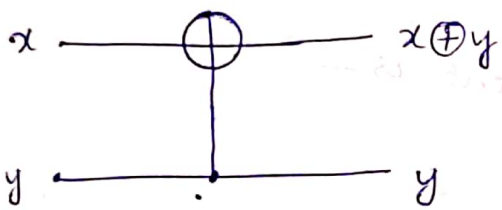
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



CNOT.

Problem-

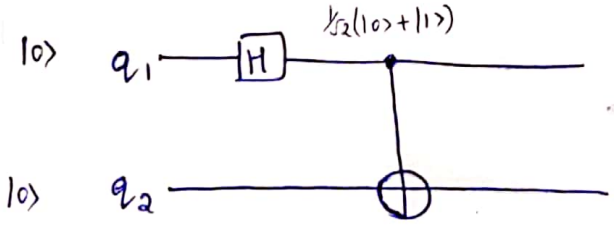
1. Find the matrix representation of the upside down CNOT-gate.



$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |11\rangle$
$|10\rangle \rightarrow |10\rangle$
$|11\rangle \rightarrow |01\rangle$

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

2. Consider the quantum circuit —



what are the outputs for the inputs $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$?

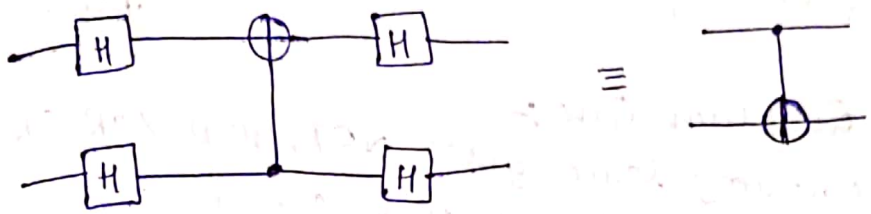
$$|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

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

} Bell states

3. Show that below circuits are equivalent.



3-qubit gates

1. Toffoli gate (Controlled-controlled-NOT or CCNOT) :-

The third input bit is flipped, if and only if the first 2 input bits are both 1.

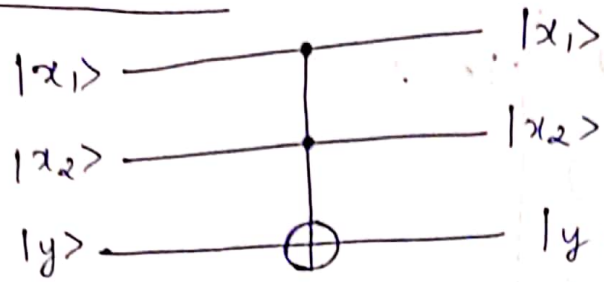
$|000\rangle \longrightarrow |000\rangle$
$|001\rangle \longrightarrow |001\rangle$
$|010\rangle \longrightarrow |010\rangle$
$|011\rangle \longrightarrow |011\rangle$
$|100\rangle \longrightarrow |100\rangle$
$|101\rangle \longrightarrow |101\rangle$
$|110\rangle \longrightarrow |111\rangle$
$|111\rangle \longrightarrow |110\rangle$

$$|000\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$|0\rangle \otimes |0\rangle \otimes |0\rangle$

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

CCNOT circuit



$x_1 x_2 = x_1 \wedge x_2$

CCNOT is universal gate and reversible gate. OR AND NAND NOR XOR are classical operation which can be implemented by using CCNOT gate.

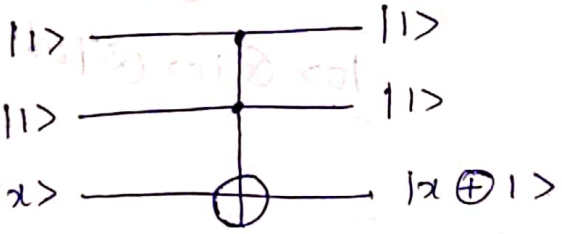
Universal Quantum Gate :-

All the elementary logic gates NOT, AND, XOR, OR NOR & NAND in classical circuits can be implemented with quantum gates. We now show that the CCNOT implements all classical logic gates.

NOT gate: The logical NOT gate is defined by

$$\text{NOT}(x) = \bar{x} = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x = 1 \end{cases}$$

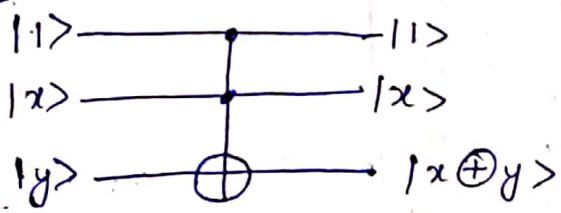
$$\text{CCNOT}\,|1\rangle\,|1\rangle\,|x\rangle = |1\rangle\,|1\rangle\,|\bar{x}\rangle$$



XOR gate : The logical XOR gate is defined by

$$\text{XOR}(x,y) = x \oplus y = \begin{cases} 0 & \text{if } x = y = 0 \text{ or } x = y = 1 \\ 1 & \text{if } x = 0\ y = 1 \text{ or } x = 1\ y = 0 \end{cases}$$

CCNOT

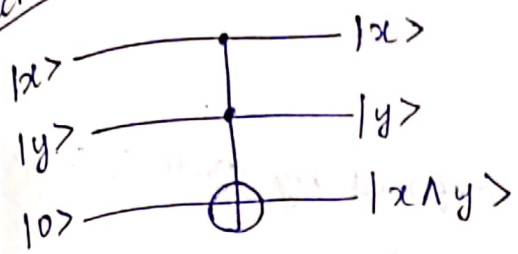


$$\text{CCNOT}\,|1\ x\ y\rangle = |1\ x\ x \oplus y\rangle$$

AND gate: The logical AND gate is defined by

$$AND(x,y) = x \wedge y = \begin{cases} 1 & x = y = 1 \\ 0 & \text{otherwise} \end{cases}$$

CCNOT



$(xy = x \wedge y)$

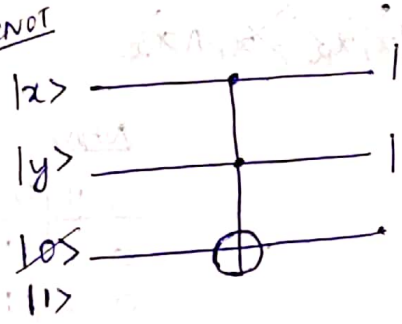
$$CCNOT\,|x\ y\ 0\rangle = |x\ y\ x \wedge y\rangle$$

OR gate: The logical OR gate is defined by

$$OR(x,y) = x \vee y = \begin{cases} 0 & x = y = 0 \\ 1 & \text{otherwise} \end{cases}$$

$$CCNOT\,|x\ y\ 0\rangle =$$

CCNOT



$$x \vee y = \overline{(\bar{x} \wedge \bar{y})}$$

$1 \oplus \bar{x}\bar{y}$

$= |x \vee y\rangle$

$|000\rangle \longrightarrow |110\rangle$

$|010\rangle \longrightarrow |111\rangle$

$|100\rangle \longrightarrow |101\rangle$

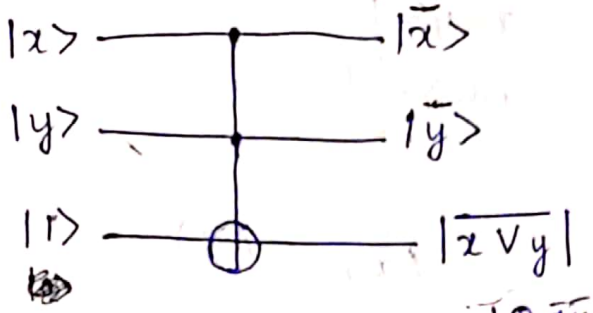
$|110\rangle \longrightarrow |111\rangle$

NOR gate:- The logical NOR gate is defined by-

$$NOR(x,y) = NOT\,(OR(x,y)) = NOT\,(x \vee y)$$

$$CCNOT\,|x\ y\ 1\rangle = |x\ y\ \overline{x \vee y}\rangle$$

CCNOT

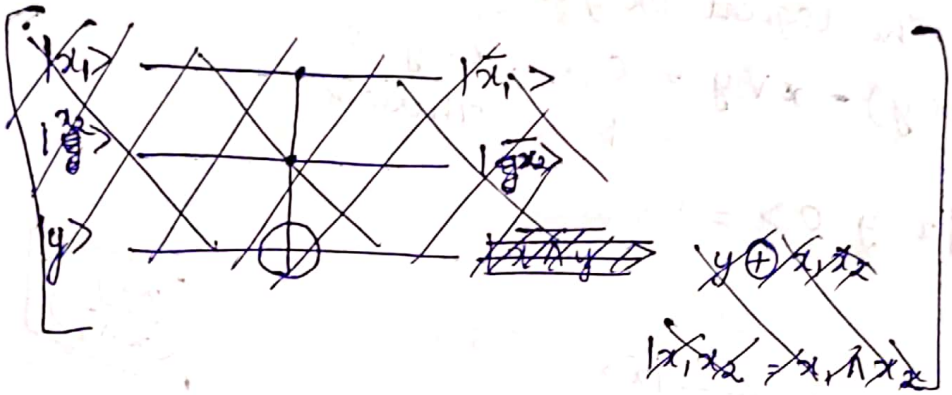


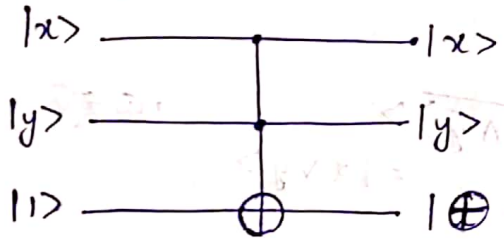
NAND gate-

The logical NAND gate is defined by NAND(x,y)

= NOT(AND(x,y)) = NOT(x ∧ y)

CCNOT |x y 1> = |x̄ ȳ $\overline{x \wedge y}$ >



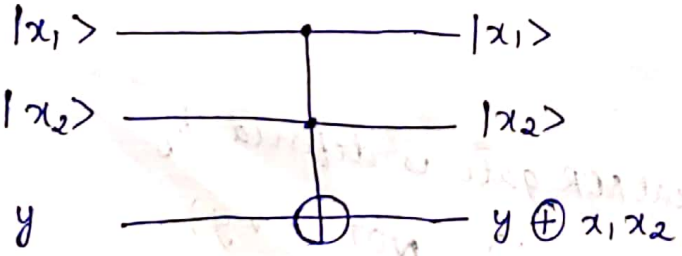


= $\overline{x \wedge y}$

NAND

x	y	o/p
0	0	1
0	1	1
1	0	1
1	1	0

CCNOT:

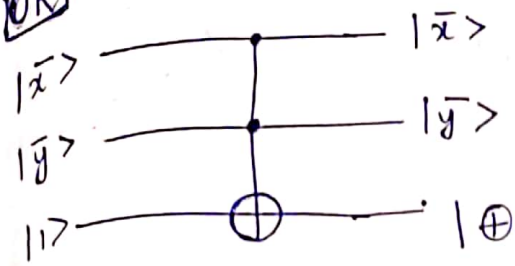


$$y \oplus x_1x_2 = \begin{cases} AND(x_1, x_2) & \text{if } y = 0 \\ XOR(y_1, x_2) & \text{if } x_2 = 0 \\ NOT\ y & \text{if } x_1 = x_2 = 1 \\ NAND(x_1, x_2) & \text{if } y = 1 \end{cases}$$

OR(x1, x2) if x1 = x̄1, x2 = x̄2 & y = 1

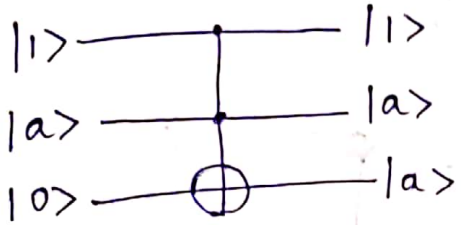
NOR(x1, x2) if x1 = x̄1, x2 = x̄2 & y = 0

OR



$= x \vee y$

Copy operation using CCNOT



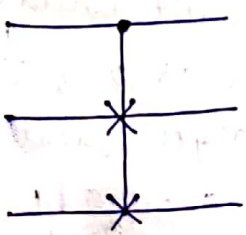
Fredkin gate (controlled-swap gate)

It swaps the values of the 2nd and 3rd bits iff the first bit is set to 1.

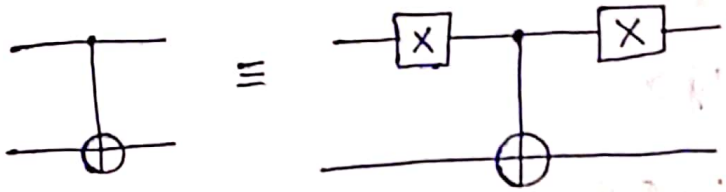
$|000\rangle \rightarrow |000\rangle$
$|001\rangle \rightarrow |001\rangle$
$|010\rangle \rightarrow |010\rangle$
$|011\rangle \rightarrow |011\rangle$
$|100\rangle \rightarrow |100\rangle$
$|101\rangle \rightarrow |110\rangle$
$|110\rangle \rightarrow 1101\rangle$
$|111\rangle \rightarrow |111\rangle$

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

C-SWAP circuit



1. Show that the two circuit below are equivalent.

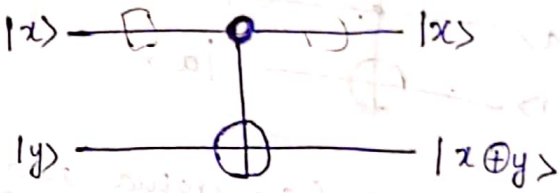


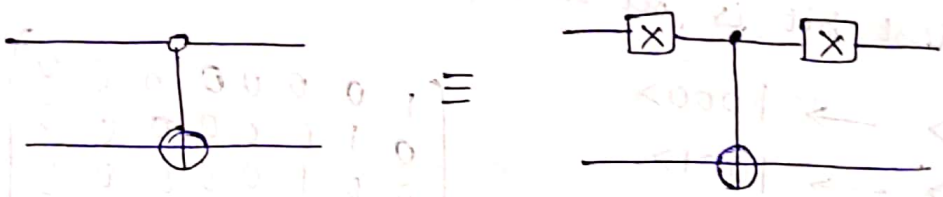
Ask Sival :p

2-qubit gate

Suppose we want to implement a 2-qubit gate in which the second (target) qubit is flipped, if first qubit (control) is set to '0'.

$|00\rangle \rightarrow |01\rangle$
$|01\rangle \rightarrow |00\rangle$
$|10\rangle \rightarrow |10\rangle$
$|11\rangle \rightarrow |11\rangle$

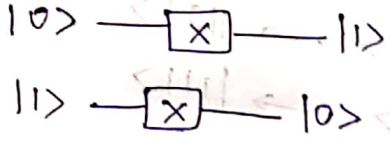




$|00\rangle \rightarrow |01\rangle$
$|01\rangle \rightarrow |00\rangle$
$|10\rangle \rightarrow |10\rangle$
$|11\rangle \rightarrow |11\rangle$

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

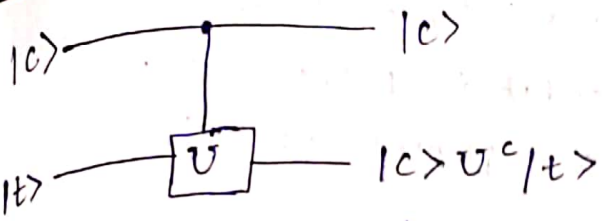
$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$



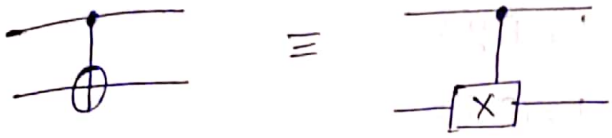
~~Compare~~

Controlled U-gate

Suppose U is an arbitrary single qubit unitary operation. A controlled-U operation is 2-qubit operation with a control and a target qubit. If the control bit is 1 then U is applied to the target bit, otherwise target bit is not changed.



C-NOT gate is same as Controlled X-gate

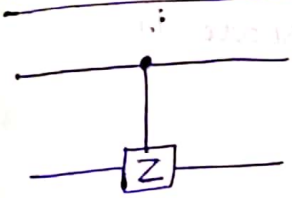


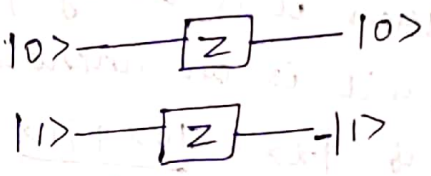
$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

≡

$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

Controlled Z-gate



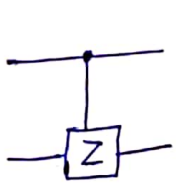


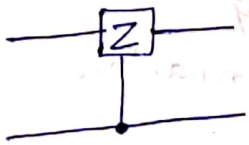
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

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

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

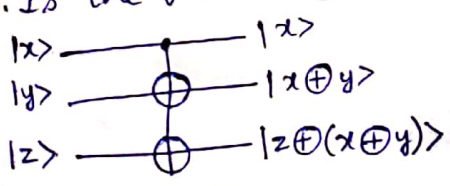
1. Is the following circuits are equivalent?

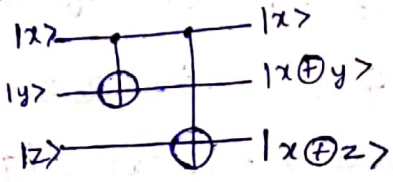




They are equivalent.

2. Is the following circuits are equivalent?

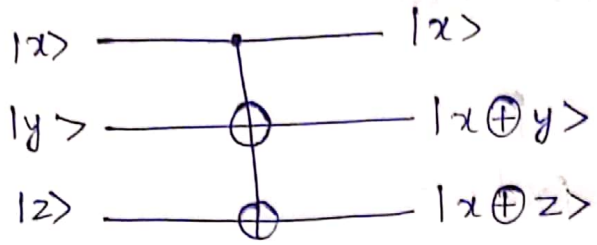




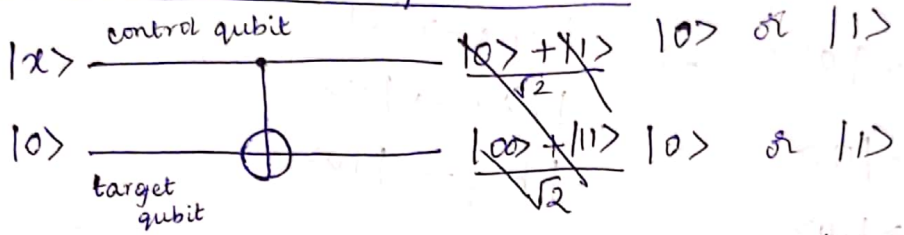
They are equivalent.

Controlled-NOT gate with multiple targets

When the control bit qubit in 1, then all the qubits marked with ⊕ are flipped, otherwise nothing happens.



No cloning with simple circuit



If qubit $|x\rangle$ is known quantum state either $|0\rangle$ & $|1\rangle$ then it is always possible to copy.

If qubit is an unknown quantum state i.e.

$$\text{if } |x\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

then at the output we will get entangled state.

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

Thus copying is not possible here.

Quantum Information Applications

We will discuss 3 protocols –

i) Quantum key distribution (QKD)

ii) Superdense coding

iii) Quantum teleportation

The one-time pad

The one time pad is defined by

$$c_i = m_i \oplus k_i, \quad i = 1, 2, 3$$

where m_i are plaintext digits –

K_i are encryption key digits

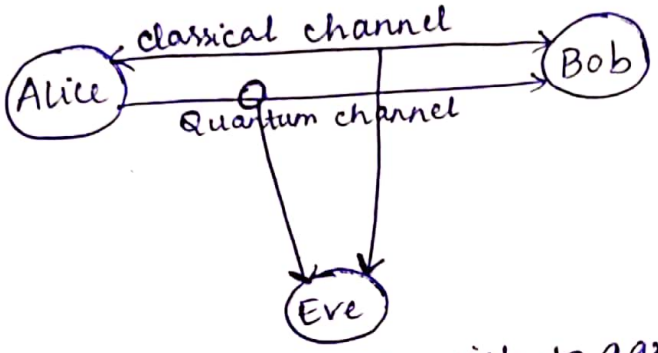
C_i are ciphertext digits

$\oplus$ XOR operation

Decryption is defined by — $m_i = C_i \oplus K_i$

QKD protocol (BB84) :-

A quantum protocol for key distribution was invented by Bennett and Brassard in 1984.



Alice and Bob wish to agree on a common key not known to Eve.

Requirements for BB84 :-

- Alice and Bob share a public authenticated classical channel.
- Alice can publically send qubits to Bob.

$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
X	H	X	H	H	X
X	H	H	X	H	H
✓	✓	X	X	✓	X