Midterm notes

Quantum Computing is an area of computer science that uses the principles of quantum theory. Quantum computing uses subatomic particles, such as electrons or photons. Quantum bits, or qubits allow these particles to exist in more than one state (i e 1 and 0) at the same time.
The power of quantum ~~computing~~ computers grows exponentially with more qubits whereas the classical computers grows linearly.

Quantum Computer vs. classical computer

→ Quantum Computer have a more basic structure than classical computers. They have no memory or processor. All a quantum computer uses is a set of superconducting qubits.

→ Quantum computers and classical computers process information differently. A quantum computer uses qubits to run multidimensional quantum algorithms. Their processing power increases exponentially as qubits are added. A classical processor uses bits to operate programs. Their power increases linearly as more bits are added. Classical computers have much less computing power.

→ Classical computers are best for everyday tasks and Quantum computers are ideal for a higher level of task eg: analyzing of data, creating energy-effecient batteries, running simulations.

→ Classical computers have low error rates and low maintanence where as Quantum computers have higher error rates and high maintanence.

Applications / Promises of Quantum Computing :-

→ Exponential information storage
  • Information is encoded through entanglement
→ Solutions to unsolved (classical) problems
→ Revolutionize cryptography
  • Threaten existing cryptographic algorithms
  • New algorithms from quantum cryptography, quantum networking
→ Brings foundational quantum mechanics to the fore
  • eg entanglement, exponential power
→ Perhaps new insights into complex algorithms and even complexity theory.

Challenges of Quantum Computation :-

→ Measurment always intrinsically disturbs the quantum system
  • Quantum systems need to be totally isolated
→ But also
  • System needs to be controlled
  • Data needs to be input and output
  • Qubits within the system need to (strongly) interact with each other
→ Quantum computers today suffer from
  • Decoherence
  • Noise

→ Must be mitigated through quantum error correction techniques.

(Qubit) A quantum bit –

- A bit of data is represented by a single quantum state (atom / electron) that is in one of two states denoted by $|0\rangle$ and $|1\rangle$ or their combination.
- A single bit in this form is known as qubit.
- A physical implementation of a qubit could use the two energy levels of an atom. An excited state representing $|1\rangle$ and a ground state representing $|0\rangle$.

Superposed Qubit – A single qubit can be forced into a superposition of the two states denoted by the addition of the state vectors:

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

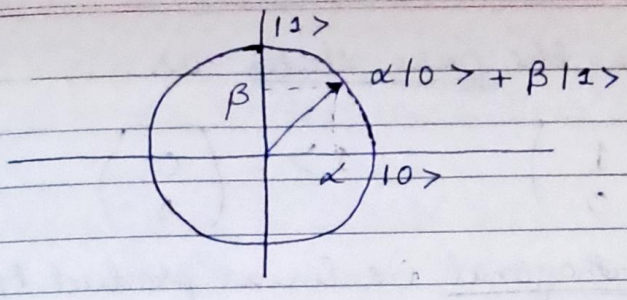
where, α and β are complex numbers

and $|\alpha|^2 + |\beta|^2 = 1$ → This normalization condition is not a property of quantum mechanics but rather of probability theory. A qubit in superposition is in both of the states $|1\rangle$ and $|0\rangle$ at the same time.

Since, the $|\Psi\rangle$ is a unit vector. Therefore

$$\langle\Psi|\Psi\rangle = 1$$

The classical bit $|w\rangle$ can be written as $|w\rangle = x|0\rangle + y|1\rangle$. The only difference is x & y are not defined over complex numbers but rather from the set $\{0,1\}$ i.e $\{x, y\} \in \{0,1\}$. The same normalization condition applies $|x|^2 + |y|^2 = 1$



Dirac Notation / bra-ket notation

bra = $\langle b|$

Ket = $|a\rangle$

A bra looks like "$\langle b|$" and mathematically it denotes a linear form $b: V \longrightarrow \mathbb{C}$, i.e, a linear map that maps each vector in V to a number in the complex plane $\mathbb{C}$.

A Ket looks like "$|a\rangle$" and mathematically it denotes a vector v in an abstract (complex) vector space V, and physically it represents a state of quantum system.

eg: $a, b \in \mathbb{C}^2$

$A^\dagger = (A^T)^*$

1) Ket $|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$

2) Bra $\langle b| = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}^\dagger$

$= \begin{pmatrix} b_1^* & b_2^* \end{pmatrix}$

3) Bra-Ket $\langle b|a\rangle$

$\begin{pmatrix} b_1^* & b_2^* \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$

$= a_1 b_1^* + a_2 b_2^*$

$= \langle a|b\rangle^* \in \mathbb{C}^2$

4) Ket-bra $|a\rangle\langle b|$

$\underset{2\times1}{\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}} \cdot \underset{1\times2}{\begin{pmatrix} b_1^* & b_2^* \end{pmatrix}}$

$= \begin{pmatrix} a_1 b_1^* & a_1 b_2^* \\ a_2 b_1^* & a_2 b_2^* \end{pmatrix}$

→ We define the pure states as

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

which are orthogonal i.e linear product of them will be 0.

$$\langle 0|1\rangle = \begin{pmatrix} 1^* & 0^* \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

where * is complex conjugate

$z = a+bi$

$z^* = a-bi$

$$= \underset{1\times 2}{\begin{pmatrix} 1 & 0 \end{pmatrix}} \cdot \underset{2\times 1}{\begin{pmatrix} 0 \\ 1 \end{pmatrix}}$$

$$= 0+0 = 0$$

→ All quantum states are normalized i.e $\langle \psi | \psi \rangle = 1$

eg: $|\psi\rangle = (|0\rangle + |1\rangle)$

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

$$\therefore \langle \psi | \psi \rangle = \begin{pmatrix} 1^* & 1^* \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

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

$$= 1+1 = 2$$

$\therefore |\psi\rangle$ is NOT normalized

Hilbert space

→ In mathematics, Hilbert spaces allow generalizing the methods of linear algebra and calculus from the

two-dimensional and three-dimensional Euclidean spaces to spaces that may have an infinite dimension.

→ A Hilbert space is a vector space equipped with an inner product operation, which allows defining a distance function and perpendicularity (known as orthogonality in this context)

→ Furthermore, Hilbert spaces are complete for this distance, which means that there are enough limits in the space to allow the techniques of calculus to be used.

eg:- The state of a vibrating string can be modeled as a point in a Hilbert space.

→ Hilbert space can finally be defined as a complex multi-dimensional space where inner product of any pair of elements is defined i.e extrapolation of a 2D space to n-dimensions and complex coefficients.

→ The state of a quantum system is defined by a unit vector in a complex, inner product space, more generally known as the Hilbert space.

Bloch Sphere is a geometric representation of a given quantum state of a qubit on the surface of a 3D unit sphere.

Bloch Sphere

→ Consider one qubit with energy eigenstates $|0\rangle$ and $|1\rangle$.

→ Putting it into superposition states:-

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

- where probability amplitudes α, β can be complex numbers
- The state must be normalized to unity so
$$|\alpha|^2 + |\beta|^2 = 1$$
- The overall phase factor has no effect, so we can choose α to be real.
- $\alpha = \cos\left(\frac{\theta}{2}\right)$ and $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$

$$|\alpha|^2 + |\beta|^2 = \cos^2\left(\frac{\theta}{2}\right) + \left(e^{i\phi}\sin\left(\frac{\theta}{2}\right)\right)^2$$

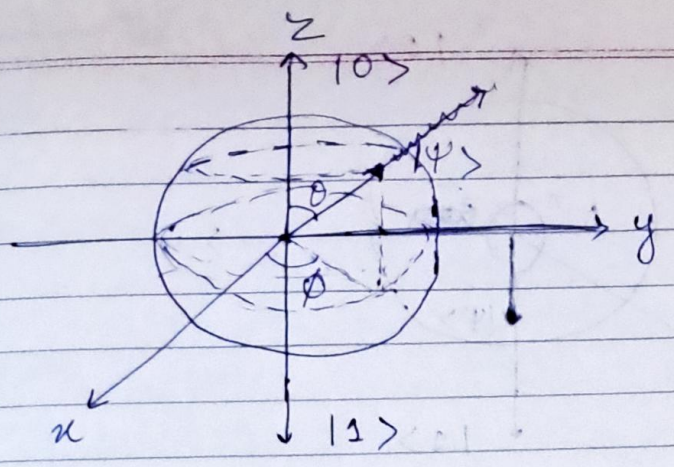
$$= \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} = 1.$$

the notation for a superposition state is:

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

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

The spher with radius of unit length is called the Bloch sphere.

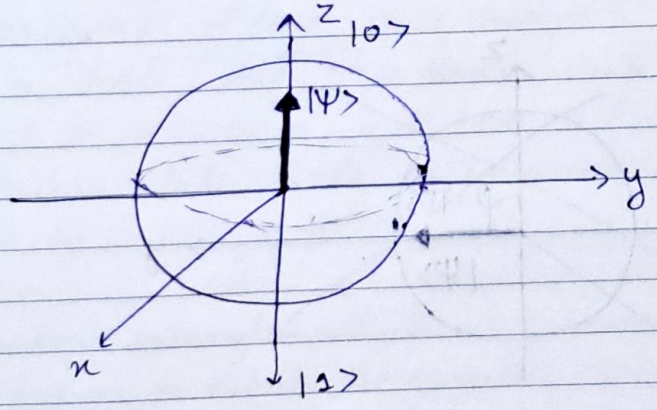


eg: when $\theta = 0$

~~$|\psi\rangle \in \cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)$~~

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

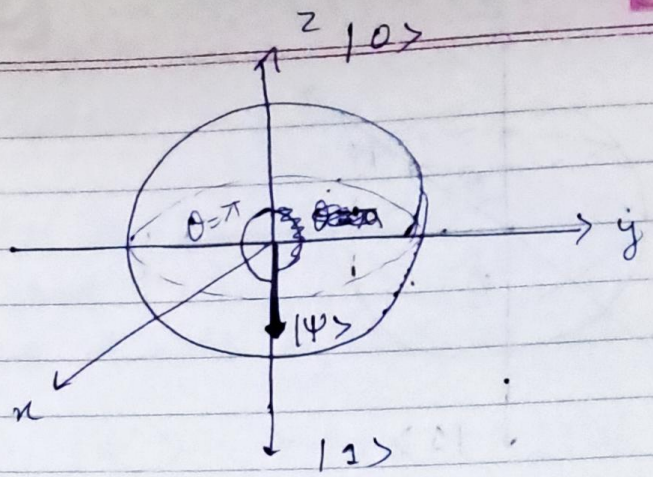
$$= |0\rangle + 0 = |0\rangle$$



eg: when $\theta = \pi$ and $\phi = 0$

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

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

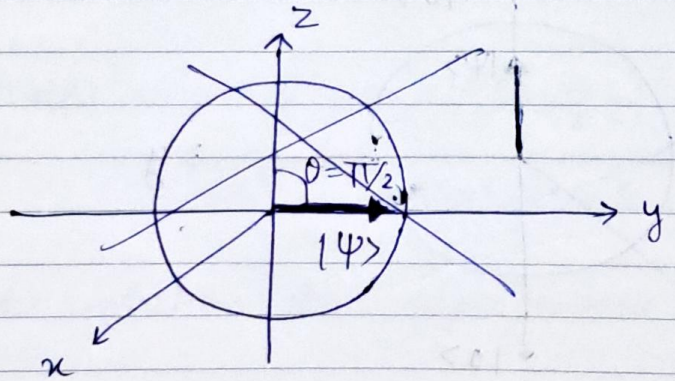


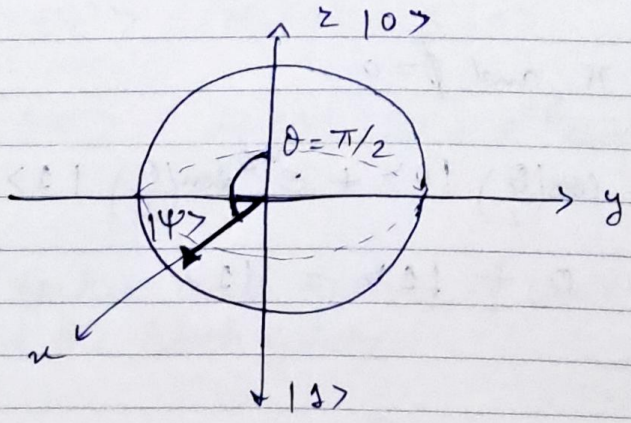
eg: when $\theta = \frac{\pi}{2}$, $\phi = 0$

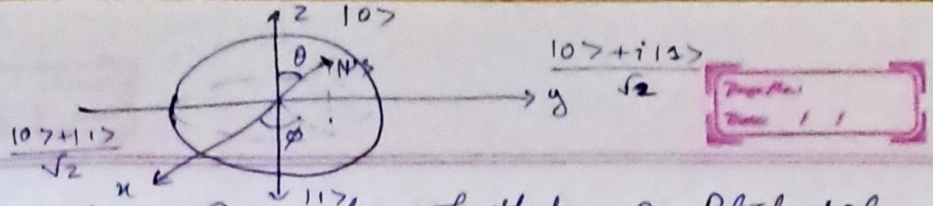
$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

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

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







→ There are ∞ number of states on Bloch sphere, but we can choose a "digital" subset for computing:

$$\Psi_0 = |0\rangle \qquad \Psi_1 = |1\rangle$$

$$|\Psi\rangle_z = |0\rangle \qquad |\Psi\rangle_{-z} = |1\rangle$$

$$\Psi_x = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad \Psi_{-x} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

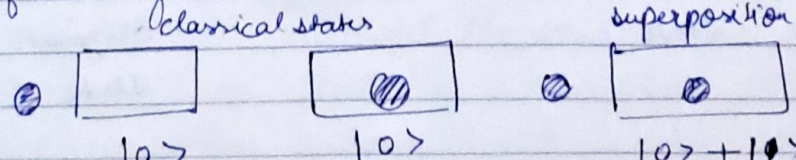
$$\Psi_y = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \qquad \Psi_{-y} = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

One classical bit (2)' possible states (0 and 1).
Two level Quantum bit.

Quantum Postulates

① Superposition of two state means a quantum systems is in two state at a time. Each superposed system, until measured, will have a finite chance of being in either state. Only when measured is it observed to be in a specific state.

② Quantum entanglement is a quantum mechanical phenomenon in which the quantum states of two or more objects have to be described with reference to each other, even though the individual objects may be spatially separated. This leads to correlations between observable physical properties of the systems.



Quantum Superposition in computing

Quantum No-Cloning theorem

→ No cloning theorem: impossible to make a (separable) copy of an unknown quantum state

→ Since we cannot mak a copy of an unknown state does not implies that the state cannot be reproduced.

→ we cannot copy qubits, but we can spread the information from a single qubit onto multiple qubits.

Theorem: There is no unitary operation U which for an arbitary state ϕ gives

$$U|\psi 0\rangle = |\psi\psi\rangle.$$

$$|0\rangle \otimes |\psi\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle$$

Blank state — State — original state

Prove:- If the above operation would have been possible then the same unitary transformation if exists, it should be able to clone any arbitary quantum state.

Considering it also true for state ϕ.

$$|0\rangle \otimes |\phi\rangle \xrightarrow{U} |\phi\rangle \otimes |\phi\rangle.$$

blank state — State — original state

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

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

$= \langle \psi | U^{+} U | \phi \rangle$ $\quad U^{+}U = I$ where U is the unitary matrix

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

$= \langle \psi\phi \rangle^{2}$

Possible only if:

- ψ and ϕ are identical
- ψ and ϕ are orthogonal.

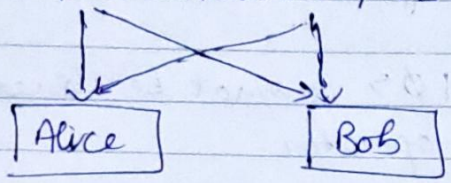
Hence, $|\psi\rangle$ and $|\phi\rangle$ cannot be cloned using any quantum unitary operator.

Teleportation / Quantum teleportation - Notion from No-cloning

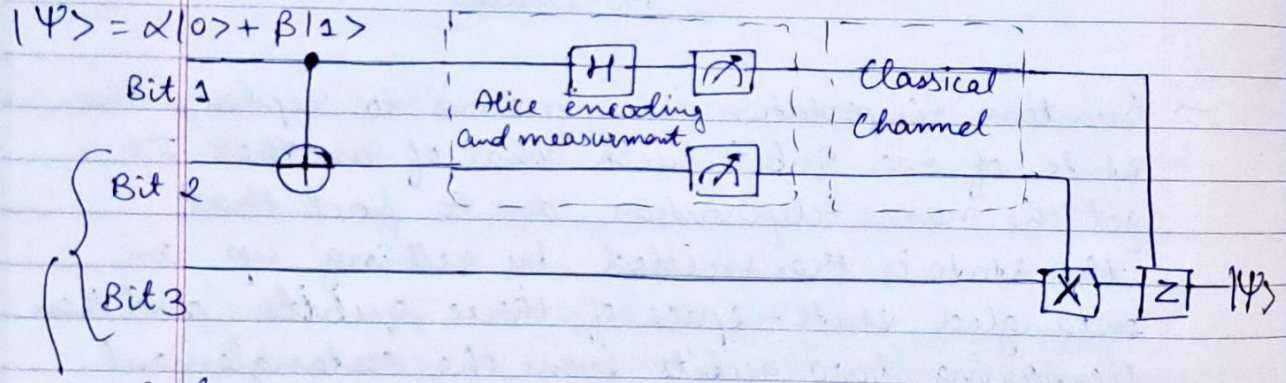
→ Quantum teleportation is a means to replace the state of one qubit with that of another. It got the name teleportation due to fact that the state is transmitted by setting up an entangled state-space of three qubits and then removing two qubits from the entanglement (via measurment).
Since, the information ~~recstate~~ of the source qubit is preserved by these measurments that information i.e state ends up in the final third, destination qubit.
This occurs without the source and destination qubit ever directly interacting. The interaction occurs via entanglement.

- Alice has a quantum state $\alpha|0\rangle + \beta|1\rangle$ which is supposed to be sent to Bob.
- Alice does not know the detailed information about the state – no measurment is possible by alice.
- Alice and Bob share one qubit each of a Bell-state, say:

$$|00\rangle + |11\rangle / \sqrt{2} \cdot \text{(an entangled state)}$$



Bit : 2 Bit : 3



Quantum teleportation circuit

Q. How far is Bob from Alice?
=> They could be separated by space-like distance.

Q. Are we able to transmit a state with a speed more than that of light?
=> This is against the theory of relativity. Quantum teleportation process incorporates transmitting a part

of classical information through a classical channel - hence, must ~~obey~~ obey relativity theory of the nature.

Q. Does Quantum teleportation means cloning the quantum state? Does it violate the "No cloning theorem"?

→ No. what alice has at her end after teleportation has become either 0 or 1 and Bob simply has recreated the state based on Alice's information

Super Dense Coding

→ Super dense coding is the less popular sibling of teleportation. It can actually be viewed as the process in reverse.

→ In Quantum teleleportation, alice has to send classical information through a classical channel and a quantum state was prepared.
In super dense coding Alice wants to send classical information, say 00, 01, 10 and 11 and she has to do this using a quantum state to send the classical information.

- Alice will be sending one bit of quantum information and Bob has to be able to extract two bits of quantum information.
~~Entangled Bell state is used as the starting point to achieve coding~~
- Alice and Bob will start with the entangled Bell pair,

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

- To send information Alice will apply unitary transformation on the first qubit of the Bell state.

00 : apply I
01 : apply X
10 : apply iY (i.e both X and Z)
11 : apply Z

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

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

$$\Rightarrow \frac{1}{\sqrt{2}}\left[I|00\rangle + I|11\rangle\right]$$

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

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

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

$$\Rightarrow \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle \right]$$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{X \otimes I}$$

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

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} |0\rangle + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} |1\rangle \right]$$

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

$$\Rightarrow \frac{1}{\sqrt{2}}\left[|10\rangle + |01\rangle\right]$$

$$\Rightarrow \frac{|10\rangle + |01\rangle}{\sqrt{2}} \qquad iY = i\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{iY \otimes I} \frac{-|10\rangle + |01\rangle}{\sqrt{2}}$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}|00\rangle + \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}|11\rangle\right]$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}|0\rangle + \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}|1\rangle\right]$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix}0\\-1\end{bmatrix}|0\rangle + \begin{bmatrix}1\\0\end{bmatrix}|1\rangle\right]$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[-|10\rangle + |01\rangle\right]$$

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \xrightarrow{Z \otimes I} \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}|00\rangle + \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}|11\rangle\right]$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}|0\rangle + \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}|1\rangle\right]$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[\begin{bmatrix}1\\0\end{bmatrix}|0\rangle + \begin{bmatrix}0\\-1\end{bmatrix}|1\rangle\right]$$

$$\Rightarrow \frac{1}{\sqrt{2}}\left[|00\rangle - |11\rangle\right]$$

- Now, Bob will apply CNOT operation

classical bits	effect CNOT of by Bob		
00	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$	$\xrightarrow{CNOT}$ $\frac{\|00\rangle + \|10\rangle}{\sqrt{2}}$	2nd qubit as 0
01	$\frac{\|10\rangle + \|01\rangle}{\sqrt{2}}$	$\xrightarrow{CNOT}$ $\frac{\|11\rangle + \|01\rangle}{\sqrt{2}}$	2nd qubit as 1
10	$\frac{-\|10\rangle + \|01\rangle}{\sqrt{2}}$	$\xrightarrow{CNOT}$ $\frac{-\|11\rangle + \|01\rangle}{\sqrt{2}}$	
11	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$	$\xrightarrow{CNOT}$ $\frac{\|00\rangle - \|10\rangle}{\sqrt{2}}$	2nd qubit as 0

In this stage Bob measures the 2nd qubit he will get either a 0 or a 1 with equal probability.

If Bob gets 0, Alice must have sent either 00 or 11.

If Bob gets 1, Alice must have sent either 01 or 10.

measurment outcom of the 1st qubit	measurmit outcome of the 2nd qubit	outcome interpretation of classical information
0	0	00
1	0	11
0	1	01
1	1	10

- Hence by sending a smaller number of quantum bits, Alice is able to communicate to Bob, a large number of classical bits.

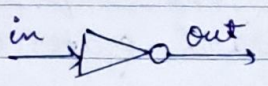
Classical vs. Quantum Logic

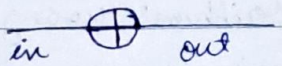
- The Goal is to have fast, low-cost implementation of useful algorithms using standard gates and design techniques
- Classical logic:
  1) Circuit behavior is governed implicitly by classical physics.
  2) Signal states are simple bit vectors eg X = 0:1010111.
  3) Operations are defined by boolean algebra
  4) No restrictions exist ~~of~~ on copying or measuring signals.
  5) Small well defined sets of universal gate types eg:- NAND, AND, OR, NOT etc.
  6) Well developed CAD methodology exist.
  7) Circuits are easily implemented in fast, scalable and macroscopic technologies such as CMOS.
- Quantum Logic:
  1) Circuit behavior is governed Explicitly by quantum mechanics.
  2) Signal states are vectors interpreted as a superposition of binary "qubit" vectors with complex number coefficients.
  3) Operations are defined by linear algebra over hilbert space.
  4) no-cloning theorem exists
  5) many universal gate sets exist but the best type are not obvious.

6) Circuits must use microscopic technologies that are slow, fragile and not yet scalable eg. NMR.

gates:-

① NOT-gate (N)





in	out
0	1
1	0

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

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

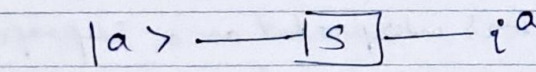
$N|0\rangle = |1\rangle$

$N|1\rangle = |0\rangle$

② ~~Reversed~~ Phase shift gate (Phase S)

The name arises because the gate shifts the phase of the $|1\rangle$ state relative to the $|0\rangle$ state.

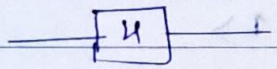
$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = T^2$$



(3) Hadamard gate

- The Hadamard gate is one of the most interesting and useful among the common gates.
- Its effect is a π rotation (half turn) in the Bloch sphere about the $\frac{\hat{x}+\hat{z}}{\sqrt{2}}$.
- In terms of Bloch sphere, hadamard gate interchages the $\hat{x}$ and $\hat{z}$ axes and inverts the $\hat{y}$ axis.

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



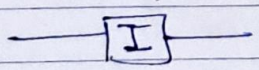
→ gives equal probabilities of $|0\rangle$ and $|1\rangle$
∴ it talks about superposition

(4) Pauli gates

- The simplest 1-qubit gates are the 4 gates represented by the Pauli operators I, X, Y, Z ($\sigma_x, \sigma_y, \sigma_z$).

(a) Pauli – I gate (Identity)

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

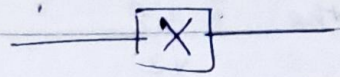


- The trivial no operation gate on 1 qubit represented by the identity matrix. Acting on any arbitrary state, the gate leave the state unchanged.

$$I|0\rangle = |0\rangle$$
$$I|1\rangle = |1\rangle$$

(b) Pauli - X gate (X gate, bit flip)

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

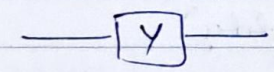


The X gate generates a half turn in Bloch sphere about the x-axis.
On computational basis, the X gate is equivalent to a NOT gate.

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

(c) Pauli - Y gate (Y-gate)

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



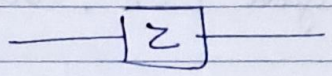
$$iY = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

The pauli Y gate generates a half turn in Bloch sphere about the y axis.
The Y gate can be thought of as a combination of X and Z gates, $Y = -iZX$

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

(d) Pauli-Z gate (Z-gate, phase flip)

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



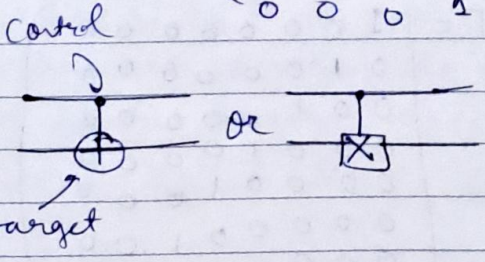
- The Pauli-Z gate generates a half turn in the Bloch sphere about the z axis
- With respect to computation, the Z gate flips the phase of the $|1\rangle$ state relative to the $|0\rangle$ state.

$$Z|0\rangle = +|0\rangle$$
$$Z|1\rangle = -|1\rangle$$

(5) Controlled-NOT gate (CNot, controlled-X, CX)

- It is also called controlled-X gate.

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



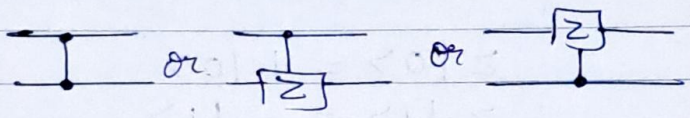
- The CNot gate is not symmetric between the two qubits. But we can switch control • and target ⊕ with local Hadamard gates.

- If control = 0 target ∅ does not flip (remains same)
  control = 1 target flips i.e 0 → 1
  1 → 0

- The control bit influences the state of the target bit, and the target bit has no influence on the state of the control bit.

(6) Controlled - Z gate (CZ, Control sign, or CSign)

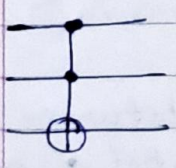
$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$



- There is no ~~control and target~~ difference between the control and target qubits.
- The CZ gate is frequently used as the elementary 2-qubit gate in circuit decompositions.

(7) Toffoli gate (Controlled Controlled NOT, CCNot, CCX gate)

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



- It is a 3-qubit gate with two control and one target qubits.
- The target bit flips only if both control bits are one.

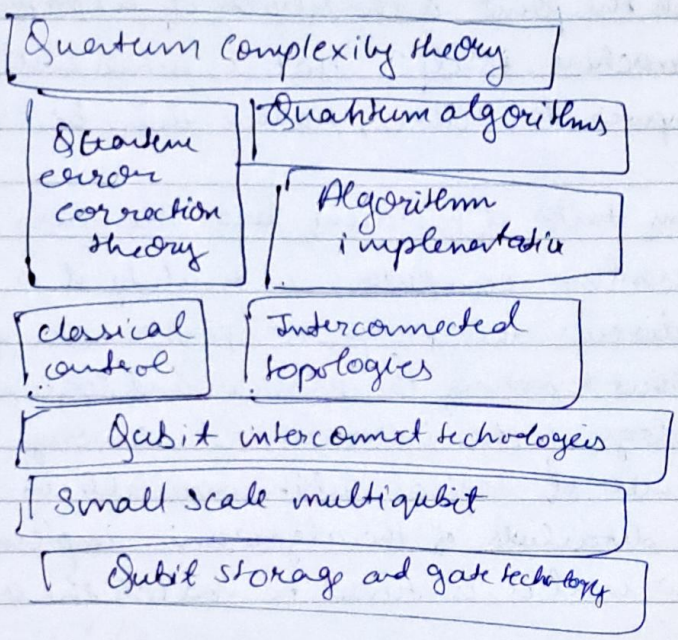
Quantum Hardware

When will the first paper appear in Science or Nature in which the point is the results of a computation, rather than the machine itself? That is when will a quantum computer do science, rather than be science?

Many talks of factoring large numbers "in seconds" using a quantum computer, in reality it is not even possible to discuss the prospective performance of a system without knowing the physical and logical clock speed, the topology of the interconnect among the qubits, the number of logical qubits available in the system, and the details of the algorithmic implementation, including how well it is tuned to match the architecture.

To actually do science with a quantum computer, we must have coordinated advances in several front.
Machines will be built to run specific algorithms.
Without the error correction the machines cannot run for any useful length of time. At the bottom of the stack lies the qubit storage, gates, interconnect technologies.
The top and bottom of the stack are heavily populated where as the middle of the stack is not that heavily populated.

A quantum computer will not make a strong distinguish between memory elements and computational elements. It uses teleportation to transfer a single qubit from ~~one~~ place to place.
The Quantum Hardware architecture differs from the von Neuman architecture



Quatum computer Architecture

(8) Controlled gates

Rx $r_x(\theta, qubit)$ $\begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$

Ry $r_y(\theta, qubit)$ $\begin{bmatrix} \cos\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$

R_z $R_z(\theta, qubit)$

$$\begin{bmatrix} e^{-i\lambda/2} & 0 \\ 0 & e^{i\lambda/2} \end{bmatrix}$$

λ = phase

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

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

(9) Phase gate

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

$$P(\lambda = \pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \text{Pauli } Z \text{ gate}$$

$$P(\lambda = \pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} = \text{Phase } S \text{ gate}$$

$$P\left(\lambda = \frac{\pi}{4}\right) = \begin{bmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{bmatrix} = T \text{ gate}$$

(10) Controlled Phase gate

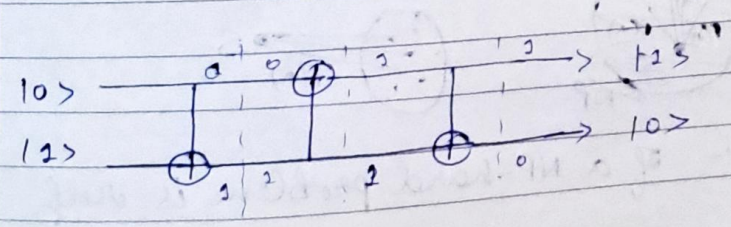
→ 2 qubit gates

$$P(\theta, qubit) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\lambda} \end{bmatrix}$$

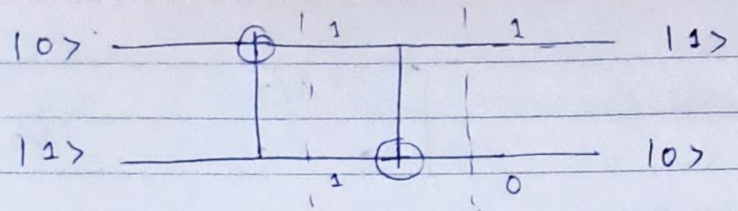
↳ CNOT

(11) Swap gate

$|01\rangle \xrightarrow{S} |10\rangle$



qiskit.org/learn

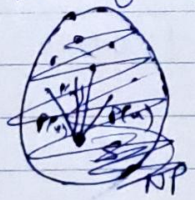


Complexity classes of Algorithms :-

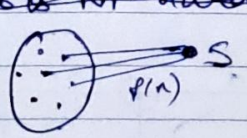
In computer Science, there exist some problems whose sol^n are not yet found, the problems are divided into classes known as complexity classes.

- P-class :- The 'P' stands for polynomial time. It is the collection of decision problem (problems with a "yes" or "no" answer) that can be solved by a deterministic algorithm in polynomial time. Also called easy problems.
- NP-class :- The 'NP' stands for Non deterministic polynomial time. It is the collection of decision problems that can be solved by a non-deterministic algorithm in polynomial time. Also called hard problems. Some problems in NP are used for cryptography.

  eg: ~~Given a number, find out its prime factors~~ factoring of a very large number is used in RSA ~~algorithm~~ encryption.
- NP-Hard :- If every problem in NP is polynomial time reducible to a problem 'S'. ~~And if S is in NP then we say that S is NP-hard. And if S is in P then we can declare that NP=P.~~

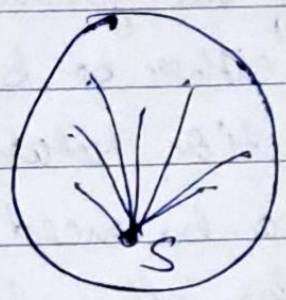


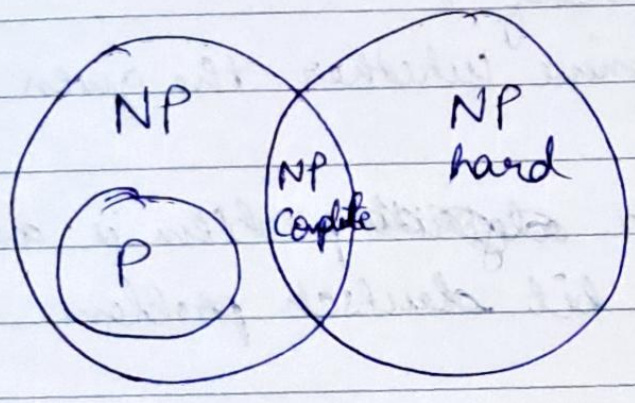
~~S is NP-hard~~



- NP-Complete :- If a NP-hard problem is itself

in NP then we say S is NP-complete. And if a NP-hard problem is P class problem then we say that NP = P





The problem of factoring a very large number say 300 digit number is solved by a classical computer in approx 1,50,000 years where as it can be solved by a quantum computer in < 1 second. This is a threat to cryptography i.e encryption scheme like RSA which uses factorization problem as its bases can be easily solved using quantum computer. Hence, we need to advance the cryptographic algorithms may be with the help of quantum computing.