Quantum Computing Easy Notes

Notes

Abhishek Bohare

a_bohare@icloud.com

typeset with LaTeX

QUANTUM COMPUTING

• Plans-

- Learning Objective
  - ~~Quantum Mechanics~~
  - Mathematical Modal of Quantum computing
  - ~~Software Engineering~~
  - Design Algorithms
  - Understanding QC
  - Principles of designing
  - QC Application limit

Quantum Algorithms

- Prerequirements-
  - Linear Algebra
  - Hilbert Space
  - Classical computing

- Examination and Self-Control
  - IVQ
  - Week tests

- Extending Knowledge
  - John Preskill's notes on QC
  - Umesh Vazirani's lectures
  - Book by David Deutsh

• Information and Computations-

Computation → A physical process
- Finite in time
- Fixed set of states

Distinguishable state → computer

Quantity of Information

$$I = -\sum_{i=1}^{n} P_i \log_b(P_i)$$

→ Physics

→ Entropy of system

$$I \Rightarrow P_i = P_j = \frac{1}{n}$$

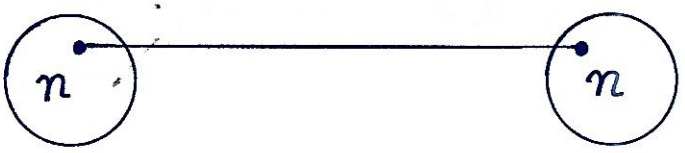
$$I = \sum_{i=1}^{n} \frac{1}{n} \log_b(n)$$

$$I = \log b^n$$

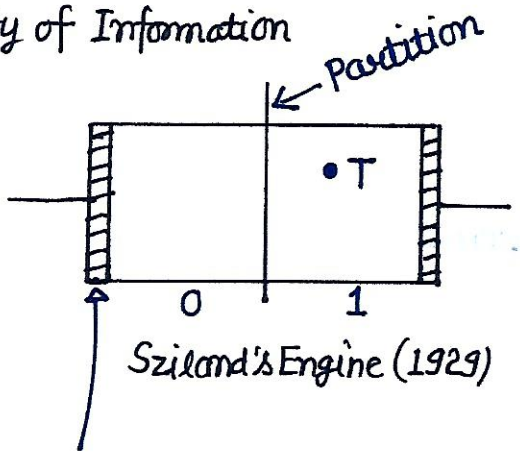
→ Matter of convension

$b=2$ $\quad \log_2 1 = 0$

$\log_2 2 = 1$, bit → Store information in bits



Quantity of Information



Assign Value 0

↓

Compress gas

$A = K_b T \ln \frac{V_1}{V_2} \Rightarrow 2$ ERASE

$A = K_b T \ln 2$

Not $0 \rightarrow 1$

Information is power.

↓

Pluto, Sucrates

↓

Modern Computers

↓

① Information Capacity (Shannon Formula)
② Speed (Switching between states)
③ Universality

↓

David Deutsh

↓

Example

↓

Rope, Steep

- Error correction
- Universality

↓

Nodes ⟶ Quality of digital systems

↓

Use this Notion

↓

Want to make base element as small as possible.

↓

- Pack more in small Volume
- Inertia, Inductance small

↓

change state

- Smaller conductors

↓

Need something else instead using PN junction

- The Goal of Computation -

- computation tranform information.
- Finding the value of some function.
- Functionshave strong mathematical definition.

$\{f : \mathbb{N} \longrightarrow (0,1)\}$

$f : \forall X \in \mathbb{N} \quad f(x)$

↓

Algorithm

•Algorithms-

- deterministic Turing Machine (DTM)
- Alan Turing
- Algorithm is finite no. of set.

⇓

Turing Thesis

↓

Turing Machine

↓

Computability

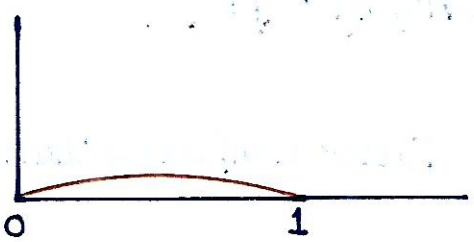
$\{f: \mathbb{N} \longrightarrow \{0,1\}\}$

↓

Some finite strings

$f: \mathbb{N} \longrightarrow \{0,1\}$

$f \quad 0, f(1)f(2)f(3)\ldots.$



↓

There are uncomputable functions.

↓

Halting Problem

H : DTM, X ⟶ { 0 , DTM stop
1 , DTM hangs

↓

Not analyzed

- Computation complexity-

- Some are easier
- Some are hard
} to compute.

- Path
  - Hamilton
  - Euler

⇓

different results for a problem

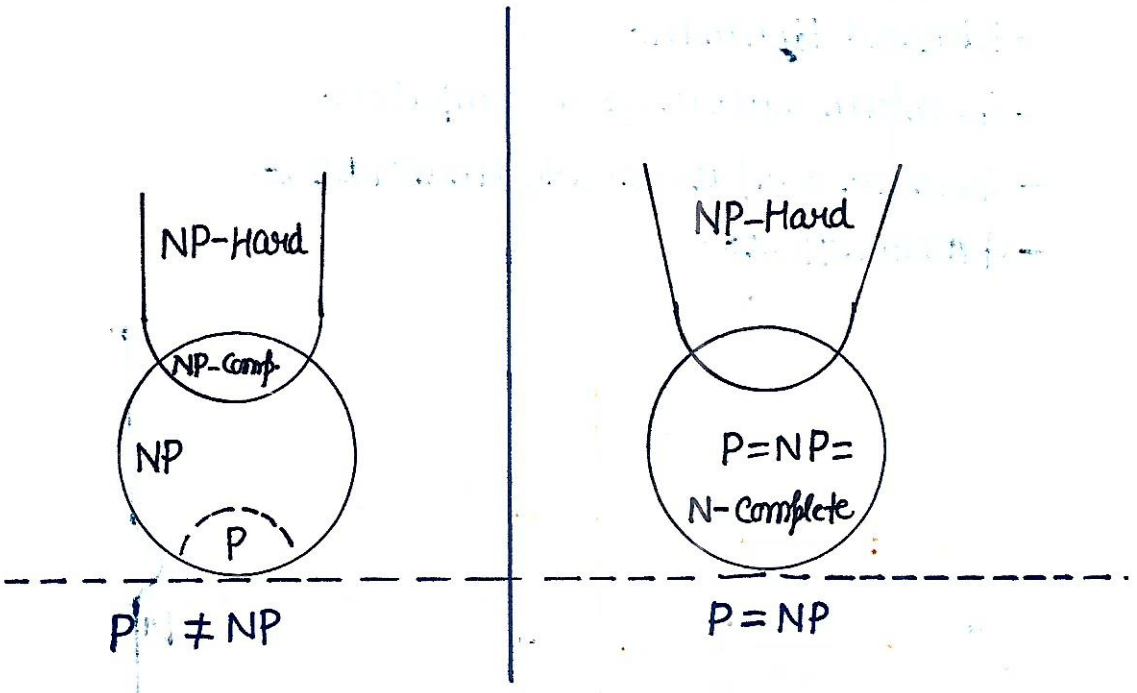
$$X + \begin{matrix} a = a_n \ldots\ldots a_1 \\ b = b_n \ldots\ldots b_1 \end{matrix} \qquad \frac{2n}{n^2}$$

⇓

Complexity in steps

$O(n)$

$O(n^2)$ Faster complexity than addition



$P \subseteq NP$

$P \subset NP$ ← Unproved

P, q 10000

$N = Pq$

↓

All algorithms

↓

Until Solar system's death

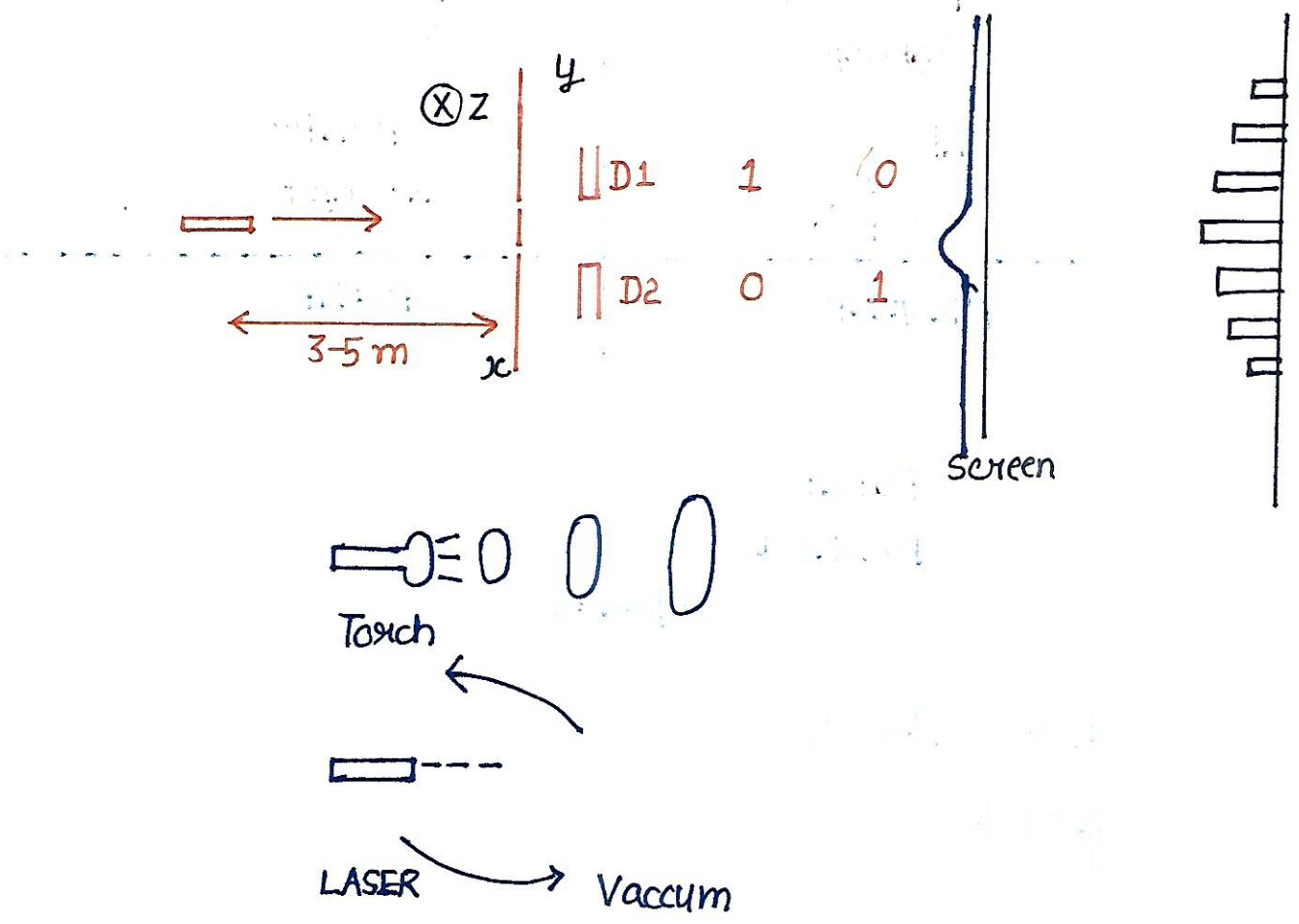
↓

Theoretically ✓

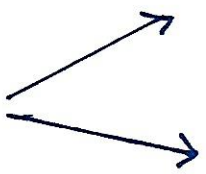
Practically ✗

• Quantum Computing -

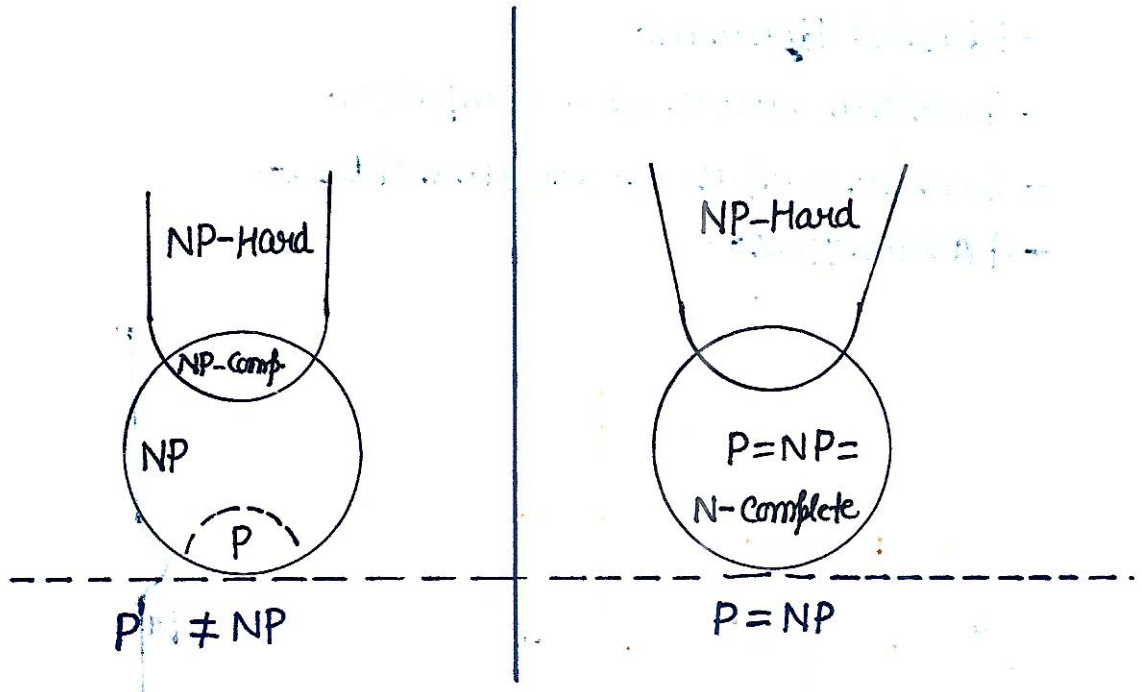
- Richard Feynman.
- Quantum system as a computer.
- Quantum computers are unavoidable.
- Quantum Effects.



- Double slit Experiment



- Two paths
- Probability distribution
- condition for particle not to collapse



$P \subseteq NP$

$P \subset NP$ ← Improved

P, q 10000

$N = Pq$

↓

All algorithms

↓

Until Solar system's death

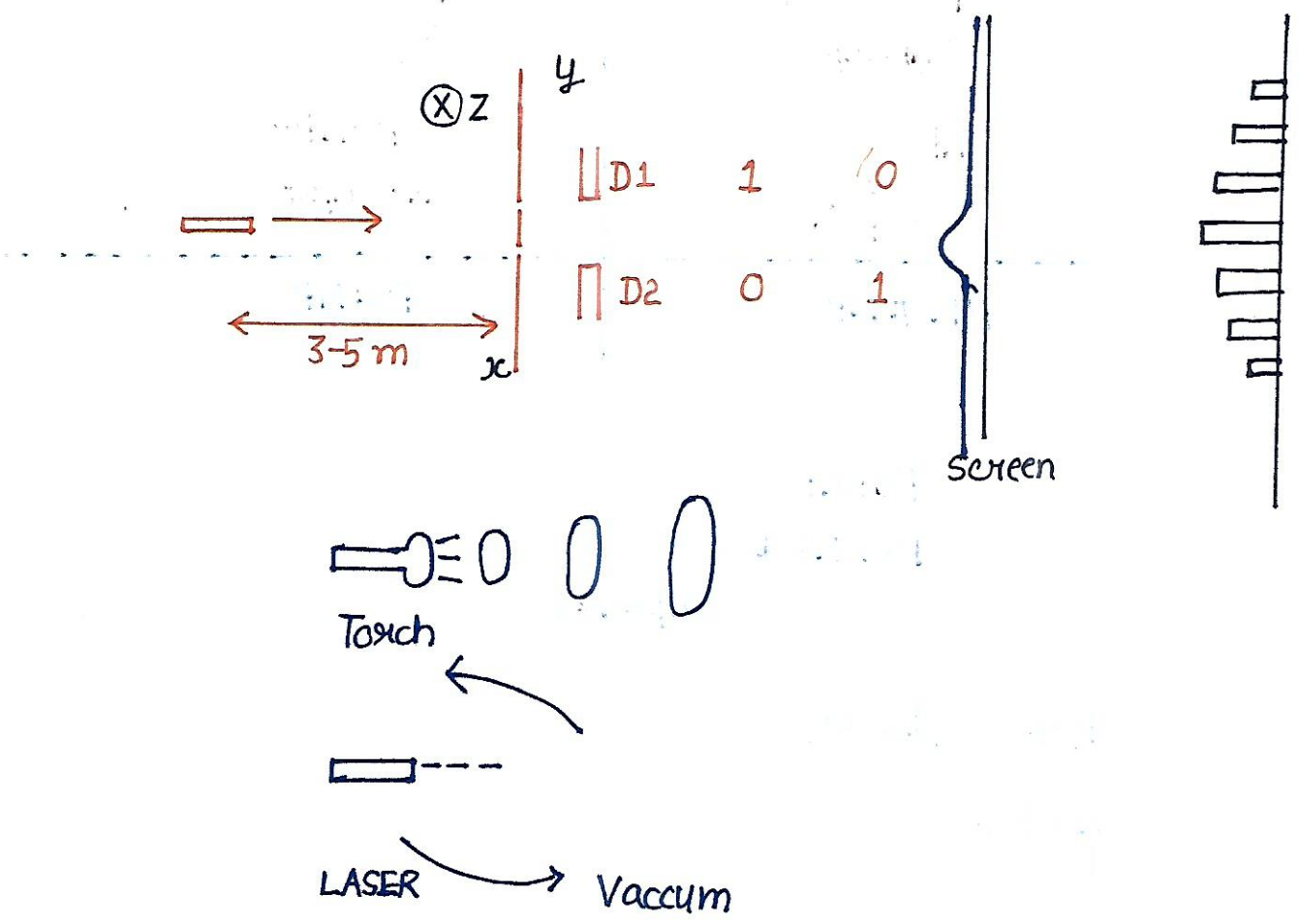
↓

Theoretically ✓

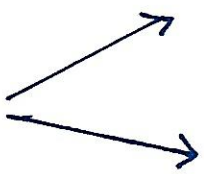
Practically ✗

• Quantum Computing -

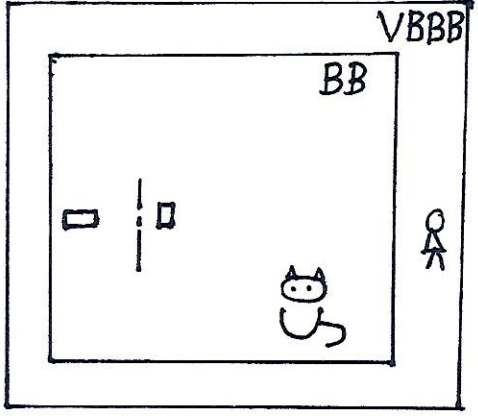
- Richard Feynman.
- Quantum system as a computer.
- Quantum computers are unavoidable.
- Quantum Effects.



- Double slit Experiment



- Two paths
- Probability distribution
- condition for particle not to collapse



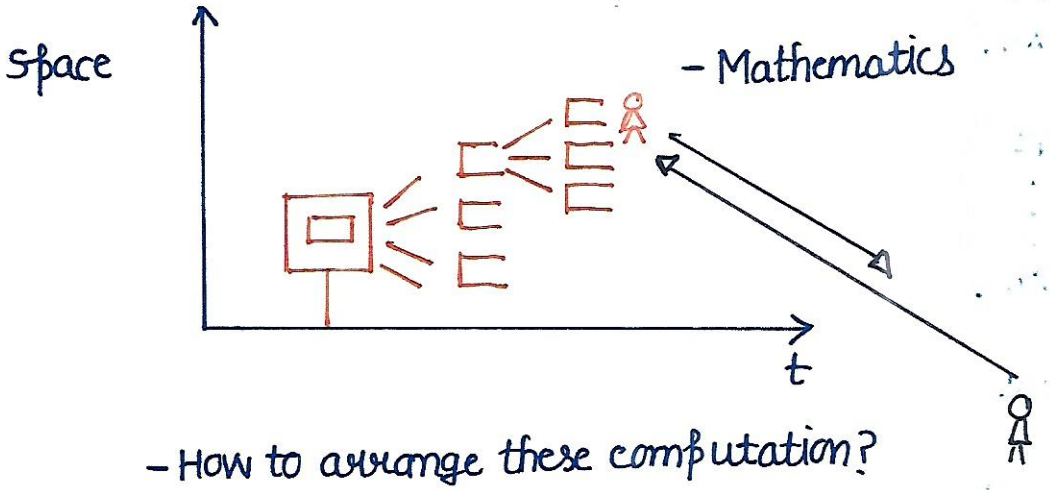
- Closed system

$|U\rangle|\uparrow\rangle + |\downarrow\rangle \longrightarrow \bullet|\downarrow\rangle + |\uparrow\rangle\bullet$ (X)

$|\text{cat}\rangle(|\uparrow\rangle + |\downarrow\rangle) \longrightarrow |\text{cat}\rangle|\downarrow\rangle + |\text{cat}\rangle|\uparrow\rangle$

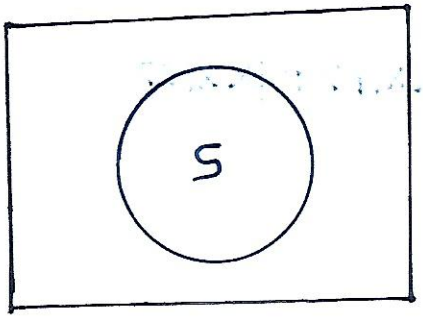
- Multiverse Interpretation of Quantum Mechanics-

  - Hugh Everett II
  - Measerement alter the wave function of the observer



- Mathematics

  - How to arrange these computation?
  - How to obtain result?

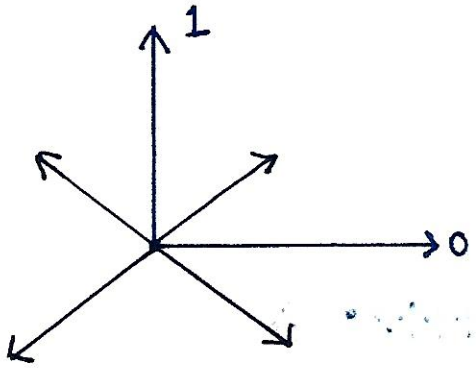


  - Interference
  - Quantum systems are hard to model.

• Mathematical Model of QC -

Qubit -

- Quantum bit



- Possible states

$|Q\rangle \in H$

$\|\phi\| = 1$

$\dim H = 2$

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$Y = \begin{pmatrix} Y1 \\ \cdot \\ \cdot \\ \cdot \\ Y_n \end{pmatrix}$$

$x_i, y_i \in \mathbb{C}$

$$\langle X|Y\rangle = \sum_{j=1}^{n} x_j^* Y_j$$

$\langle X|X\rangle \geq 0$

$\langle X|\alpha y + \beta z\rangle = \alpha\langle X|Y\rangle + \beta\langle X|z\rangle$

$$|X\rangle = \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}$$

$\langle X| = (x_1^* \ldots\ldots x_n^*)$

$$\frac{\langle x|y\rangle}{\|x\|\|y\|} = \cos\alpha \qquad [0,\pi]$$

$$[0, \tfrac{\pi}{2}]$$

$$\cos\theta = |\langle x|y\rangle|$$

$$\theta = \arccos|\langle x|y\rangle|$$

$$|x\rangle \perp |y\rangle (=) \langle x|y\rangle = 0$$

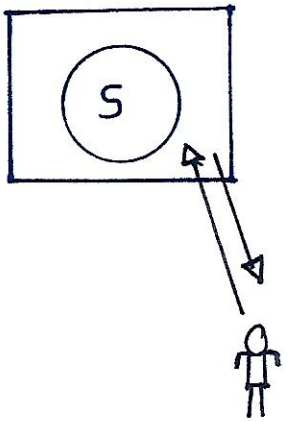
$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

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

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

$$\alpha, \beta \in \mathbb{C}$$

Quantum Measurement-



$$|\text{🧍}\rangle(|s_1\rangle + |s_2\rangle) \longrightarrow |\text{🧍}\rangle|s_1\rangle + |\text{🧍}\rangle|s_2\rangle$$

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

$$P(|0\rangle) = |\alpha|^2$$
$$P(|1\rangle) = |\beta|^2$$

$\cos\theta = \langle 0|\phi\rangle = \langle 0|\alpha|0\rangle + \beta|1\rangle\rangle = \alpha\langle 0|0\rangle + \beta\langle 0|1\rangle = |\alpha|$

$P(|0\rangle) = \cos^2\theta$

$P(|1\rangle) = \sin^2\theta$

$|\text{Q}\rangle|0\rangle + |\text{Q}\rangle|1\rangle + \ldots\ldots$

Possibilities

Other possibilities

- The Measurement is a probabilistic system.
- Copying of unknown quantum states are impossible.

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

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

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

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

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

$|+\rangle = |\phi\rangle$

$|-\rangle = |\phi\rangle$

Systems with Multiple qubit-

$|0\rangle, |1\rangle$

qubit I	qubit II
$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$

qubit I	qubit II
$\|0\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$

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

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

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

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

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

$\rightarrow |01\rangle = |0\rangle\otimes|1\rangle$

$\rightarrow |10\rangle = |1\rangle\otimes|0\rangle$

$\rightarrow |11\rangle = |1\rangle\otimes|1\rangle$

$n \longrightarrow 2^n$ $\quad n = 1$

$\Rightarrow 2^1$

$\Rightarrow 2$

$\Rightarrow 4$ $\quad n = 2$

$\Rightarrow 8$ $\quad n = 4$

$\Rightarrow 1024$ $\quad n = 10$

$\Rightarrow 2^{1000} \sim 10^{300}$ $\quad n = 1000$

Measuring the multiple qubit system-

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

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

Quantum Evolution-

$$UU^* = U^*U = I$$

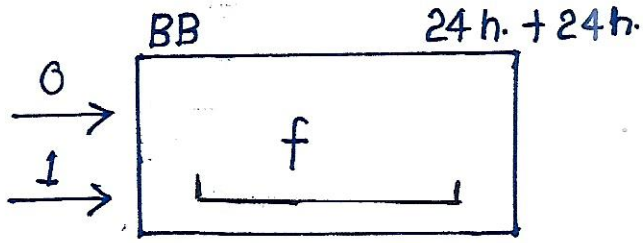
#Quantum Computer and Algorithms-

- Deutsch's Problem-

$$f : \{0,1\} \longrightarrow \{0,1\}$$

$f(x) = 0$, $f(x) = 1$] constant

$f(x) = x$, $f(x) = \bar{x}$] Balanced



$$U|f\rangle \longrightarrow |f(x)\rangle$$

$f = 0$

$U|f\rangle = |0\rangle$

$$U_f |x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$$

$$|00\rangle \longrightarrow |0\, f(x)\rangle$$

$$|10\rangle \longrightarrow |1 f(x)\rangle$$

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

$$= \frac{1}{\sqrt{2}} \left(U|x\rangle f(x)\rangle - |x\rangle|1 \otimes f(x)\rangle\right)$$

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

$f(x) = 0$

$U_f |x\rangle|y\rangle \longrightarrow |x\rangle|y \otimes \overset{0}{f(x)}\rangle = |x\rangle|y\rangle$

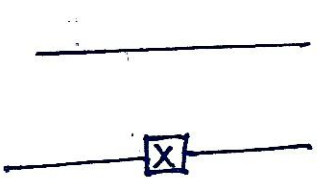
$U_f = I$ 4x4

$f(x)=0$

$U_f = I$

$f(x)=1$

$U_f|x\rangle|y\rangle \longrightarrow |x\rangle|y \otimes 1\rangle$



$$\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} = I \otimes X$$

$f(x)=x$

$|00\rangle = |00\rangle$

$|01\rangle = |01\rangle$

$|10\rangle = |11\rangle$

$|11\rangle = |10\rangle$

$U_f = CNOT$

$f(x)=\bar{x}$

$|00\rangle = |01\rangle$

$|01\rangle = |00\rangle$

$|10\rangle = |10\rangle$

$|11\rangle = |11\rangle$

$$\begin{pmatrix} X & 0 \\ 0 & I \end{pmatrix}$$

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

$$|01\rangle \xrightarrow{H} \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)$$

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

$$\xrightarrow{U_f} \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle-|1\rangle) + \frac{1}{2}(-1)^{f(0)}|1\rangle(|0\rangle-|1\rangle)$$

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

f = Constant

$f(0) = f(1)$ $\quad |+\rangle$

$f(0) \neq f(1)$ $\quad |-\rangle$

We don't know which will stay as result

- Quantum compater-
  - Entanglement
  - Qubit 1 ⟶ Photon
  - Qubit 2 ⟶ Polarization

Quantum oracle

$$U_f = \frac{1}{\sqrt{2}}(-1)^{f(x)}|x\rangle(|0\rangle-|1\rangle)$$

- Quantum Computer prototype –
  - Interferometer
  - Real Quantum computer

- More Algorithms –

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

$$|x : f(x)=1| = |x : f(x)=0|$$

$$|0\rangle^n |1\rangle \xrightarrow{H^{n+1}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$$

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

$$= H^n |0\rangle^n$$

$|00\ldots.0\rangle$

$$\frac{1}{2^{n/2}} \left(\sum_{x:f(x)=0} |x\rangle - \sum_{x:f(x)=1} |x\rangle \right)$$

$$H|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle$$

Factoring and Other factors in Shor's Algorithms -

- Factoring and RSA -

- Polynomial time algorithms for discrete logarithms and factoring on a quantum computer.

$P \neq q$
$N = Pq$
> Prime Problems

- Find P and q

$2 .. \sqrt{N}$

- RSA

https

↓

1973 by Clifford Cocks

↓

Importance of RSA

↓

Encryptions / Decryptions / Data Security

- RSA Algorithm -

$N = Pq \quad \forall a < N : (a, N) = 1$

$a^{\phi(N)} = 1(N)$

$\psi(N) = \psi(Pq) = (P-1)(q-1)$

$\psi(P) = P-1$

$\psi(q) = q-1$

$e < N, (e, N) = 1, (e, \phi(N)) = 1$

$ed = 1(\phi(N))$

$ed + \phi(N)K = 1$

Artificial Intelligence

Week 4
1. 2^{365}
2. 14
3. 30^{10}

Week 4
1. 991
2. Yes, It is.
3.
4. No
5. BACDB / BADCB
6. 15 BDCAB

Week 4
1. 19
2. 2311
3. 1,3,4
4. 0
5. 14

(e,N) Public Key
(d,N) Private key

$(m,N) = 1$
(e,N)

$m^e(N)$
$(m^e)^d(N) = m^{ed}(N)$
$ed = 1 + \varphi(N)k$
$m \cdot m^{\varphi(N)k}(N) = m(N) = m$

$\Rightarrow$ $P = 11$
$q = 13$

$N = 11 \cdot 13 = 143$
$\varphi(N) = 10 \cdot 12 = 120$

$e = 17$
$m = 7$
$(17, 143)$

$7^{17}(143) = 7(49)^8(143) \Rightarrow /2401(143) = 113(\ldots)/$
$= 7(113)^4(143) = 7(42)^2(143)$

$113 = -30(143) = 900(143) = 42(143)$

- Are quantum computers always better?

  - Quantum computers are always better.
  - But there are some exception cases.