20/02/25

For 3-Qubits

Oracle

Oracle known	
000	0
001	1
010	0
011	0
100	0
101	0
110	0
111	0

lookup table

$$H(000) = \frac{1}{(\sqrt{2})^3}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)$$

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

$$= \frac{1}{2\sqrt{2}}(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle + |101\rangle+|110\rangle+|111\rangle)$$

$$H(001) = \frac{1}{2\sqrt{2}}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)(|0\rangle-|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle+|001\rangle+|010\rangle-|011\rangle+|100\rangle - |101\rangle+|110\rangle-|111\rangle)$$

$$H(010) = \frac{1}{(\sqrt{2})^3}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)(|0\rangle+|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle+|001\rangle-|010\rangle-|011\rangle + |100\rangle+|101\rangle-|110\rangle-|111\rangle)$$

$$H(011) = \frac{1}{(\sqrt{2})^3}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)(|0\rangle-|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle-|001\rangle-|010\rangle+|011\rangle + |100\rangle-|101\rangle-|110\rangle+|111\rangle)$$

$$H(100) = \frac{1}{2\sqrt{2}}(|00\rangle+|01\rangle-|10\rangle-|11\rangle)(|0\rangle+|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle+|001\rangle+|010\rangle+|011\rangle - |100\rangle-|101\rangle-|110\rangle-|111\rangle)$$

$$H(101) = \frac{1}{2\sqrt{2}}(|00\rangle+|01\rangle-|10\rangle-|11\rangle)(|0\rangle-|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle-|001\rangle+|010\rangle-|011\rangle - |100\rangle+|101\rangle-|110\rangle+|111\rangle)$$

$$H(111) = \frac{1}{2\sqrt{2}}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)(|0\rangle-|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle-|001\rangle-|010\rangle+|011\rangle-|100\rangle+|101\rangle + |110\rangle-|111\rangle)$$

$$H(110) = \frac{1}{2\sqrt{2}}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)(|0\rangle+|1\rangle)$$

$$= \frac{1}{2\sqrt{2}}(|000\rangle+|001\rangle-|010\rangle-|011\rangle - |100\rangle-|101\rangle+|110\rangle+|111\rangle)$$

lookup table

	000	001	010	011	100	101	110	111
000	1	1	1	1	1	1	1	1
001	1	−1	1	−1	1	−1	1	−1
010	1	1	−1	−1	1	1	−1	−1
011	1	−1	−1	1	1	−1	−1	1
100	1	1	1	1	−1	−1	−1	−1
101	1	−1	+1	−1	−1	+1	−1	+1
110	1	1	−1	−1	−1	−1	1	1
111	1	−1	−1	1	−1	1	1	−1

$\psi_1 = |000\rangle|1\rangle$

$\psi_2 = \frac{1}{(\sqrt{2})^3} \sum_{x=0}^{7} |x\rangle(|-\rangle)$

$\Rightarrow \frac{1}{\sqrt{8}}\left(|0\rangle+|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle\right)$

$\psi_3 = \frac{1}{\sqrt{8}}\left(|0\rangle-|1\rangle+|2\rangle+|3\rangle+|4\rangle+|5\rangle+|6\rangle+|7\rangle\right)$

Before look up table

ψ_4 →	000	001	010	011	100	101	110	111
000	+	1	+	+	+	1	+	+
001	+	1	+	+	−	1	−	−
010	1	+	+	+	+	1	−	−
011	1	−	+	+	−	−	−1	−
100	1	+	+	1	−	1	−1	+
101	1	−	+	−	−	1	+	−
110	1	+	−1	+	−1	−	−	1
111	1	−	−1	1	−1	+	+	−
	6	2	−2	2	−2	2	−2	2

$\Rightarrow \frac{1}{2\sqrt{2}}\left(6|0\rangle+2|1\rangle-2|2\rangle+2|3\rangle-2|4\rangle+2|5\rangle-2|6\rangle+2|7\rangle\right)$

$\Rightarrow \frac{1}{\sqrt{2}}\left(3|0\rangle+|1\rangle-|2\rangle+|3\rangle-|4\rangle+|5\rangle-|6\rangle+|7\rangle\right)$

$|\psi_5\rangle \Rightarrow$

$\Rightarrow \frac{1}{\sqrt{2}}\left(3|0\rangle-|1\rangle+|2\rangle-|3\rangle+|4\rangle-|5\rangle+|6\rangle-|7\rangle\right)$

ψ_6 →	000	001	010	011	100	101	110	111
000	+	1	+	+	+	+	+	−
001	−	1	−	+	−	+	−	+
010	+	1	−	+	+	+	−	−
011	−	1	+	−	−	+	+	+
100	+	+	+	+	−	−	−	−
101	−	1	−	1	+	−	+	−
110	+	1	−	+	−	−	+	+
111	−	1	1	−	+	−	−	+

$\Rightarrow \frac{1}{\sqrt{2}}|4\rangle$

$\Rightarrow \frac{1}{\sqrt{2}}|1\rangle$

$\Rightarrow \sqrt{2}|1\rangle$

$\downarrow$

ψ.

Here, the Qubit ψ is $|1\rangle$.

Shor's Algm → Measure prime factorization

- Very popular
- DFT → Very popular in signal processing ~~signals~~ opns.
  - extensively used
  - for faster computation faster FTs.
  - FT transform time domain to frequency domain
  - reversible. $t \to f$, $f \to t$
    - w/o any loss, we can get the original domain.

eg. for 1D signal → speech → function of time

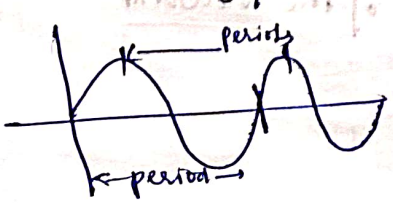
- 2D " → Image viewed as sliced version of 1D signal [unit-width]. 2D → 1D
  - So we can use FT.

⇒ To remove the noise → FT is used.

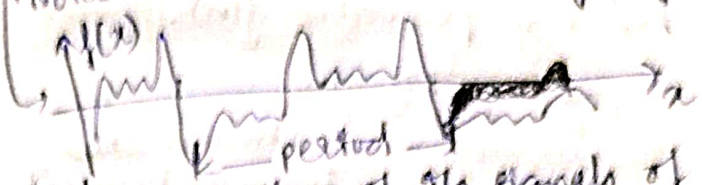
- Speech is very low freq → 8 Hz.
  - but Jan sound → 20 KHz.
  - ↳ we take freq domain, remove all the high freq and convert back to time domain.
- It is reversible [lossless].

Discrete Fourier Transform (DFT)

≈ in QC → QFT (Quantum Fourier Transform)



- Speech is an example of periodic.
- Noise is not characterized by any regularity



↳ Composition of ip signals of several frequencies.

- Every signal has a periodicity

$f: \{0,1\}^n \to \{0,1\}^m$

$f(x) = f(x+kp)$

$k \in Z - \{0\}$

$f(x) = f(x+p)$

$\to f(x+2p) \cdots$

② Periodic finding algm

③ Shor's Algm

Primitive roots of Unity

$z^n = 1$ z is a Complex Number

Find its n roots.

Its n roots are

$\{w_n^0, w_n^1, w_n^2 \cdots, w_n^{n-1}\}$

where $w_n^k = e^{2\pi i \frac{k}{n}}$ ← all the roots lie on the unit circle.

Properties

Property-1

① w_n^k lie on the unit circle

$|w_n^k| = 1$

$|w_n^k| = e^{2\pi i \frac{k}{n}} \cdot e^{-2\pi i \frac{k}{n}}$ ← same thing is applied here

$= e^0 = 1$

② Eg: $|1+i| = \sqrt{(1+i)(1-i)} = \sqrt{2}$

require searching

Property-2:

w_n^k is a periodic f(n).

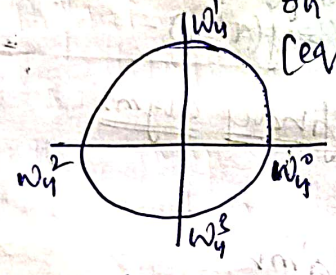
$w_n^k = w_n^{k \bmod n}$ ← this makes the root bounded within a given range.

Eg①:

Q. $4^4 = 1$

The roots are

$\{w_4^0, w_4^1, w_4^2, w_4^3\}$ ← all of them lie on unit circle [equidistant].



from the formula,

$$w_n^k = e^{2\pi i \frac{k}{n}}$$

$w_4^0 - k=0 = e^{2\pi i \cdot \frac{0}{4}} \Rightarrow e^0 = 1$

$w_4^1 = k=1 = e^{2\pi i \cdot \frac{1}{4}} \Rightarrow e^{\frac{i\pi}{2}} = i$

$w_4^2 - k=2 = e^{2\pi i \cdot \frac{2}{4}} \Rightarrow e^{i\pi} = -1$

$w_4^3 - k=3 = e^{i2\pi \cdot \frac{3}{4}} \Rightarrow -i$

$\{1, i, -1, -i\}$

↳ Rearrange

$\Rightarrow \{1, -1, i, -i\}$

$w_4^4 = w_4^{4 \bmod 4} = w_4^0$

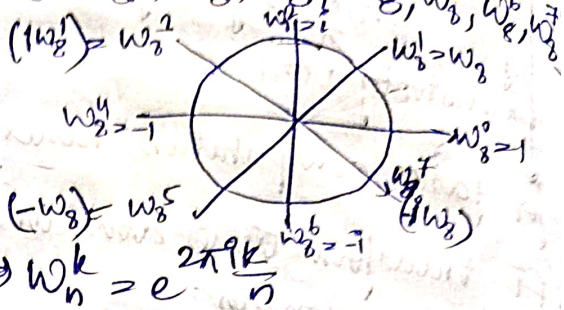
$\Rightarrow w_4^7 = w_4^3$

Eg②:

Q. Find roots of $z=8$.

The roots are

$\{w_8^0, w_8^1, w_8^2, w_8^3, w_8^4, w_8^5, w_8^6, w_8^7\}$



$\Rightarrow w_n^k = e^{2\pi i \frac{k}{n}}$

$\Rightarrow w_8^0 \rightarrow k=0 \Rightarrow e^0 = 1$

$\Rightarrow w_8^1 \rightarrow k=1 = e^{2\pi i \cdot \frac{1}{8}} = e^{\frac{\pi i}{4}} = \frac{1+i}{\sqrt{2}}$

$\Rightarrow w_8^2 - k=2 = e^{2\pi i \cdot \frac{2}{8}_4} = e^{\frac{\pi i}{2}} = i$

$= w_8^3 - k=3 = e^{i2\pi \cdot \frac{1}{8}_4} = e^{\frac{3\pi i}{4}} =$

$= w_8^4 - k=4 = e^{2\pi i \cdot \frac{4}{8}_2} = e^{i\pi} = -1$

$= w_8^5 - k=5 = e^{2\pi i \cdot \frac{5}{8}_4} = e^{i\frac{5\pi}{4}_2}$

$= w_8^6 - k=6 = e^{2\pi i \cdot \frac{6}{8}_2} = e^{i\frac{3\pi}{2}} = -i$

$= w_8^7 - k=7 = e^{2\pi i \cdot \frac{7}{8}_4} = e^{i\frac{7\pi}{4}_2}$

$\Rightarrow \boxed{w_8^3 = (w_8^1) \cdot i}$

So, roots are

$\{1, w_8, i, \bar{w}_8, -1, -w_8, -i, \bar{w}_8\}$

- There is a QC for QFT. and Eq'lent matrix form.

DFT Matrix:

- nxn matrix

Elements of the matrix:

$$\frac{1}{\sqrt{n}}\begin{bmatrix} w_n^{0\times0} & w_n^{0\times1} & \cdots & w_n^{1\times(n-1)} \\ w_n^{1\times0} & w_n^{1\times1} & & \\ \vdots & & & \\ w_n^{(n-1)\times0} & w_n^{(n+1)\times1} & \cdots & w_n^{(n-1)\times(n-1)} \end{bmatrix}_{n\times n}$$

If $n=4$

$\hookrightarrow w_4^{3\times2} = w_4^{9} = w_4^{1}$

Transformation means changing a coordinate w.r.t changed axes. Here, time domain is transformed.

Transform

$|\psi\rangle = \frac{|0\rangle + |3\rangle}{\sqrt{2}}$ Using f_4.

$\Rightarrow f_4|\psi\rangle$

$$\Rightarrow \frac{1}{\sqrt{4}}\begin{bmatrix} w_4^{0\times0} & w_4^{0\times1} & w_4^{0\times2} & w_4^{0\times3} \\ w_4^{1\times0} & w_4^{1\times1} & w_4^{1\times2} & w_4^{1\times3} \\ w_4^{2\times0} & w_4^{2\times1} & w_4^{2\times2} & w_4^{2\times3} \\ w_4^{3\times0} & w_4^{3\times1} & w_4^{3\times2} & w_4^{3\times3} \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} w_4^0 & w_4^0 & w_4^0 & w_4^0 \\ w_4^0 & w_4^1 & w_4^2 & w_4^3 \\ w_4^0 & w_4^2 & w_4^4 & w_4^6 \\ w_4^0 & w_4^3 & w_4^6 & w_4^9 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} w^0 & w^0 & w^0 & w^0 \\ w^0 & w^1 & w^2 & w^3 \\ w^0 & w^2 & w^4 & w^6 \\ w^0 & w^3 & w^6 & w^9 \end{bmatrix}$$

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

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

$f_4|\psi\rangle = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}_{4\times4} \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}_{4\times1}$ for $0 \le x \le 3$ (1)

↳ these both will be multiplied. coz of this

$$\Rightarrow \frac{1}{2\sqrt{2}}\begin{bmatrix} 1+1 \\ 1-i \\ 1-1 \\ 1+i \end{bmatrix}$$

$$\hookrightarrow \frac{1}{2\sqrt{2}}\begin{bmatrix} 2 \\ 1-i \\ 0 \\ 1+i \end{bmatrix}$$

$$\Rightarrow \frac{1}{2\sqrt{2}}\left[2|0\rangle + (1-i)|1\rangle + 0|2\rangle + (1+i)|3\rangle\right]$$

$$\Rightarrow \frac{2}{2\sqrt{2}}|0\rangle + \frac{(1-i)|1\rangle}{2\sqrt{2}} + \frac{(1+i)|3\rangle}{2\sqrt{2}}$$ ⇒ Here this should be normalised then

⇒ We know that when we try to measure a quantum state, it collapses.

- $|0\rangle$ is the o/p with prob $\frac{1}{2}$
- $|1\rangle$ is " $\frac{1}{4}$
- $|3\rangle$ is " $\frac{1}{4}$

coz it can't be in imaginary.

Sum of the probabilities $= 1 \neq 1$

⇒ Then the original states are not in normalized state.

24/02/25

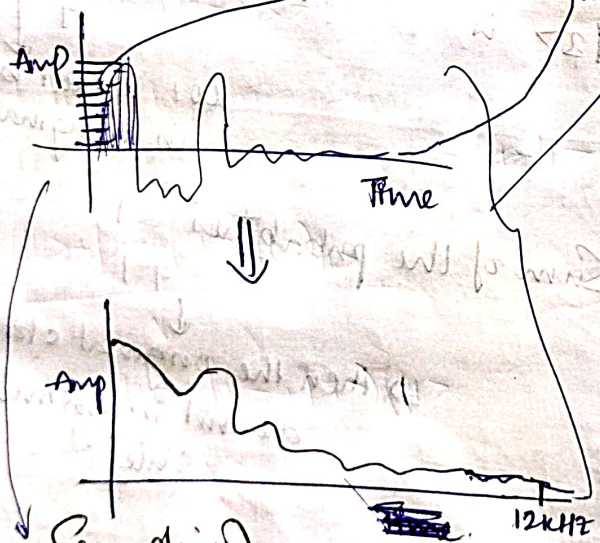
- In nature, every action, phenomenon etc is Analog.
- Earlier 1970's comp. → Analog
  - computation challges
  - storage "
- So, switched to digital
- As time passed, Analog clocks disappeared / perished.

1) Analog signal → Sampling
2) to Digital done by 2 steps → Quantization

- from the given signal, highest freq. component is selected.

Eg: Diff. freq. components
↳ diff magnitude

Some are dominant / less dominant



- If Sampling doesn't be compromised. If highest is 12KHz, if we sample at the rate 2×12 = [24KHz] per sec, means that close samples are collected at close intervals.
  ↳ lossless operation.

- Means 24KB is being assigned per 1 sec
  ↳ Costly.
- If we want to preserve as it is
  ↳ Costly.

⇒ 24K × 1 bytes ⇒ 96 KB/sec
↓ per min ×60.
⇓
↑ Complexity.

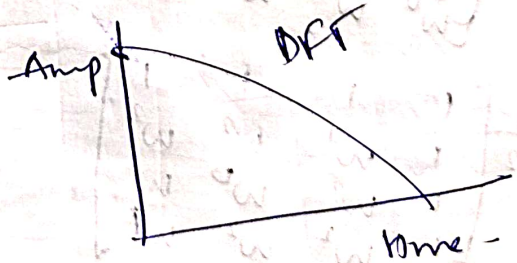
Quantization → lossy.
↳ Instead of 4 bytes, we can get 8 bits, → 2^8 ⇒ 8 levels.
, So, a point based on that level can be quantized.

⇒ Analog → Digital

- Whenever we record, rest all are high freq, speech is low freq.
  ↓
  4KHz – reasonably good
  8KHz – very good.

passed through low-pass filter
↳ low
↳ high → discarded.

↓
New Signal
[In this higher freq is only there – 4KHz].
↕
DFT



- To save the bw, all the signals are passed through lowpass filters
  then → Sampling
  ↳ Quantization.

x. Processing of image >>> Imaging DBMS

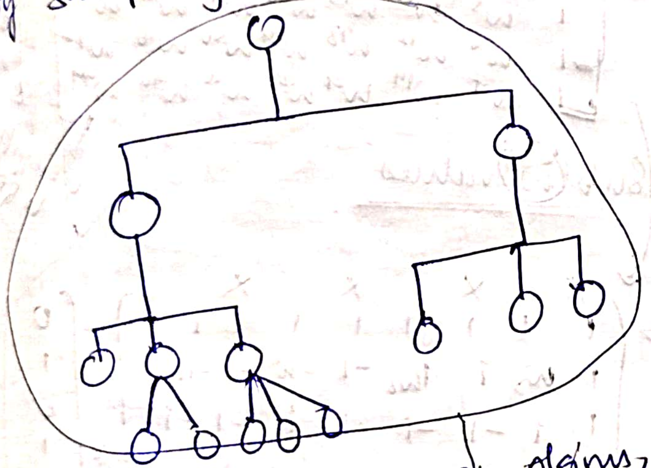
lossy — Non lossy → expensive

Some of the info not even available in signal but found in FT.

FT is a reversible/revokable operation

time → freq (⟷), w/o any loss

But Analog → DFT [Irrevokable], because some info is lost at quantization stage[lossy], no effect by sampling[lossless].



· Here, we didn't use ML algms, but at one place we have to use DL, ML Algm, whole soln becomes irrevokable → Changes the entire characteristic

· If bits are ↑ also, error ↓ but error can't be made 0.

(4) Period finding algo

· ML Algms are working 90% cor,

In nature everything is periodic, if there is no periodicity → if humans only can't → Machines also can't.

→ So, there shld be implicit periodicity in the problem statement → is → not perceived by humans,

⇒ so asking ML Algms to find.

Q. find period r in the given function

$f : \{0,1\}^3 \rightarrow \{0,1\}^3$

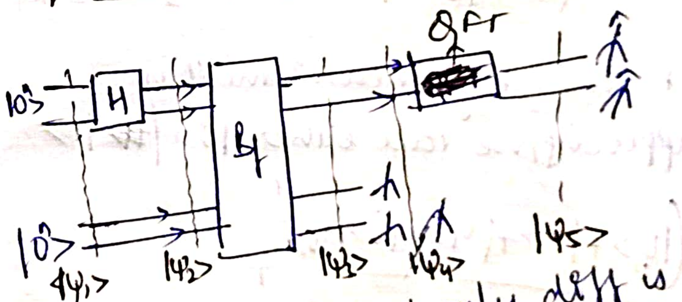
where, $f(x) = x \bmod 2$

x	0	1	2	3	4	5	6	7
y	0	1	0	1	0	1	0	1

Range = 8

Sol: Here, period is 2.

Quantum Circuit for this Qr



· function ≅ to U_f but only diff is for U_f → 2nd o/p is 1, but in B_f all are 0

· In this circuit, there are 2 registers each consisting of 'n' Qubits, total consisting of '2n' Qubits.

· At $|\psi_3\rangle$, we are terminating and moving ahead by making a small change

$n=3$

$|\psi_1\rangle = |0^n\rangle|0^n\rangle = |000\rangle|000\rangle$

$|\psi_2\rangle = H^{\otimes 3}|0^3\rangle = |0^3\rangle$

$= \frac{1}{\sqrt{2^3}} \sum_{x=0}^{7} |x\rangle |000\rangle$

$= \frac{1}{\sqrt{8}} (|0\rangle + |1\rangle + \cdots + |7\rangle)|000\rangle$

$n+n$

By $|x\rangle|0\rangle = |x\rangle|f(x)\rangle$

earlier,

$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$|\psi_3\rangle = \frac{1}{\sqrt{8}} (|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \cdots + |7\rangle|f(7)\rangle)$

$= \frac{1}{\sqrt{8}} (|0\rangle|0\rangle + |1\rangle|1\rangle + |2\rangle|0\rangle + \cdots + |7\rangle|7\rangle)$

Now refer to the prev. table

$= \frac{1}{\sqrt{8}} ((|0\rangle + |2\rangle + |4\rangle + |6\rangle)|0\rangle + (|1\rangle + |3\rangle + |5\rangle + |7\rangle)|1\rangle)$

• At this stage, measurement is happening, we take either $|0\rangle$ / $|1\rangle$

$\Rightarrow \frac{(|0\rangle + |2\rangle + |4\rangle + |6\rangle)}{\sqrt{8}}|0\rangle + \frac{(|1\rangle + |3\rangle + |5\rangle + |7\rangle)}{\sqrt{8}}|1\rangle$

Case-1:

let $|1\rangle$ is measured by DFT.

• we shld 1st normalise it.

$\frac{1}{\sqrt{8}} (|1\rangle + |3\rangle + |5\rangle + |7\rangle) \cdot |1\rangle$

$\frac{(|1\rangle + |3\rangle + |5\rangle + |7\rangle)}{\sqrt{4}}$

Case-2:

let $|0\rangle$ is measured by DFT

$\frac{1}{\sqrt{8}} \frac{(|0\rangle + |2\rangle + |4\rangle + |6\rangle)}{\sqrt{4}} \cdot |0\rangle$

$|\psi_5\rangle = QFT_8 |\psi_4\rangle$

large

[shld be atleast equal to 1 complete cycle of we ↑ → robustness ↑.

Case-1:

$|\psi_5\rangle =$

$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_8^1 & \omega_8^2 & \omega_8^3 & \omega_8^4 & \omega_8^5 & \omega_8^6 & \omega_8^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\ 1 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\ 1 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49} \end{bmatrix} \frac{1}{\sqrt{4}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$

corresponding to $|1\rangle$

Sub. $\omega^{\frac{n}{8}}$ values

$= \frac{1}{\sqrt{4}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega_8 & i & i\omega_8 & -1 & -\omega_8 & -i & -i\omega_8 \\ 1 & i & -1 & -i & 1 & i & -1 & -1 \\ 1 & i\omega_8 & -i & \omega_8 & -1 & -i\omega_8 & i & -\omega_8 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\omega_8 & -i & -i\omega_8 & -1 & \omega_8 & -i & -i\omega_8 \\ 1 & -1 & -1 & +1 & \omega_8 & -\omega_8 & -\omega_8 & \omega_8 \\ 1 & -i\omega_8 & -i & -\omega_8 & -1 & +i\omega_8 & i & \omega_8 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$

$\Rightarrow \frac{1}{4\sqrt{2}} \begin{bmatrix} 4 \\ 0 \\ 0 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \frac{1}{\sqrt{2}} (|0\rangle - |4\rangle)$

For case-2:

$\Rightarrow \frac{1}{\sqrt{2}} (|0\rangle + |4\rangle)$

this means $|0\rangle$ & $|4\rangle$ with equal probability, so anything can be taken. This shld be done for logn times, for more robustness. ↓ Here 0,4 and compute GCD of all potential candidates

Now we have → GCD(0,4) ⇒ (4).

⇒ Period required is r.

N → samples

$\frac{N}{r} = 4 \Rightarrow \frac{8}{r} = 4$

$r = 2$

↓

period of $f(n)$ is 2.

from table [prev page].

$f(0) = f(2) = f(4) = f(6) = 0$ Ufy

$f(1) = f(3) = f(5) = f(7) = 1$.

- QFT is not a mathematical step, we can generate a circuit for this also.
  → this is outcome of another circuit called QF circuit.

5/03/25

Goal of Shor's Algm to find u & v such that $N = u \times v$.

If u & v are primes → only one soln ↓ such nos are used in cryptography.

Modulus Arithmetic

⇒ $20 \equiv 2 \pmod 3$

$2 \equiv 20 \pmod 3$

$(20 \bmod 3) \equiv 2$

congruent

Divisibility

- If a is completely divisible by N, then $a \equiv 0 \pmod N$.

Eg: $32 \equiv 0 \pmod 2$ → 2 divides 32 completely.

Order

Given N, x then

r is the smallest +ve no such that $x^r \equiv 1 \pmod N$, if this condn is satisfied, then 'r' is called order.

- The key idea is:

$$x^r - 1 \equiv 0 \pmod N$$

⇒ LHS → we are subtracting 1.

$$(x^{r/2})^2 - 1^2 \equiv 0 \pmod N$$

$$(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod N$$

⇒ LHS is written as 2 factors, means even factor gives remainder → 0.

N → given
x → assumed
r → computed

} in a problem.

↳ we will explore 'r' values [from 1 - ↳ Brute force

Trivial Solutions

$x^{r/2} = \pm 1$

Non-Trivial Solutions

$x^{r/2} \neq \pm 1$

⇒ In Shor's algm, we are interested in

$(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod N$

$a \cdot u \quad b \cdot v$

if $\gcd(x^{r/2} - 1, N) = u$ → But this is simple

then $v = \frac{N}{u}$

$\gcd(x^{r/2} + 1, N) = v$

Shors Algm resembles RSA, but only diff is ~~same~~ can be represented as Quantum Circuit.

Shors Algorithm Steps:

While(true){

1. Choose $x \in \{2, N-1\}$ → gcd=1 denotes both the args are prime nos.
2. If ($d = gcd(x, N) \geq 2$) then $\{u = d, v = N/u\}$
3. Find r such that $x^r \equiv 1 \pmod N$

// Here r is found using a Q.C of order finding Algm //.

4. If (r is even && $d = gcd(x^{r/2} - 1, N) \geq 2$)
   return u=d, v=N/u;

}

. We are looking for ~~gnt~~ factors not real values

happen only when (r) is even

Find the factor of N=21.

Sol: $x^r - 1 \equiv 0 \pmod{21}$

we can take $x \in \{2, 20\}$

① If x=5

2. gcd(21,5) = 1 ✗

3. $5^r \equiv 1 \pmod{21}$

⇒ choose another 'x' val. is answer is ✗

r=1 $5 \equiv 5 \bmod 21$

r=2 $5^2 \equiv 4 \bmod 21$

$5^3 \equiv 20 \bmod 21$

$5^4 \equiv 16 \bmod 21$

$5^5 \equiv 17 \bmod 21$

$5^6 \equiv 1 \bmod 21$

$gcd(5^{6/2} - 1, 21)$

$gcd(125 - 1, 21)$

$gcd(124, 21) = 1$

So change (x)

② Choose another x.

i) x = 8

ii) gcd(21,8) = 1

r=1 ⇒ $8 \equiv 8 \bmod 21$

$8^2 \equiv 1 \bmod 21$ [can stop here]

extra: $8^3 \equiv 10 \bmod 21$

$8^4 \equiv$

$gcd(8^{2/2} - 1, 21) \Rightarrow 7$

u = 7, v = 21/7 = 3

⇒ Always a successful search but a lot of overhead due to brute force computations.

Order:

Repeating itself with a period

r =	1	2	3	4	5	6
$x^r \bmod N$ = 8	1			1		1

↓ there is a period

⇒ This is done by Q.C by order finding algm.

for all algos like Deutsch-Josha, Grover, etc - Oracle knows the solu
but we repeat for N, √N times etc,
why?
↳ we need to extract it from

↳ this is not studied in any other computry.

Some philosopheres say humans are unbuilt intelligence, this research is to retreive that

charles Babbage
↳ Father of CS
↓
he gave 1st schematic diagram of computer
↓
no more valid for QC's.
[there is no separate MUnit in QC]

⇒ See 6/01/25
↳ we shld belive that QC is Det & embibe that into our lives.

7/03/25

- ALU & CU are integral part of system.
what is the need for understandg Proteomics & Genomics?
- Biology is very imp for replicatg/ understandg QC in a better way like computation, diff regulations.
- If you want for QC, some regulations of Biology shld be incorporated.

- Cell - self
- One of the majr activity of cell is Protein Synthesis.
- As far as routine activities in cell, it is done everyday.
- How this is actually done?

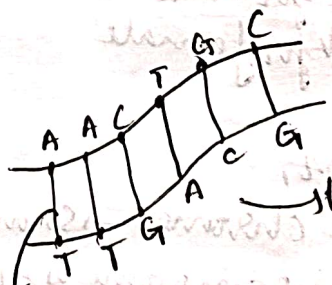
37 trillion cells
↓
1 cell = 3 billion base pairs.

⇒ 

DNA

DNA - 3×10^9 bpairs → 6 billion molecule
[ATGC]
↓
Each base is a molecule
↓
A - Adenine - $C_5H_5N_5$
T - Thymine - $C_5H_6N_2O_2$
G - Guanine - $C_5H_5N_5O$
C - cytosine - $C_4H_5N_3O$
every molecule has $C_4H_1N_1O$ atoms.
↓
has no 'O' - is an exception cas

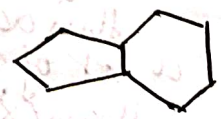
A - T
C - G



→ helical shape.

base pair

→ Purine (A, G) | Pyramidine (T, C)



Genomics & Proteomics

→ omics ⇒ Understanding the computations.
↳ [regulatory complex]

· When we want to design a system, to embibe this regulatory we should understand the nature.

Nucleoside — Base + Sugar
[A, T, G, C] ↳ one of them

↗ Stable, intelligent

Nucleotide — Base + Sugar + Phosphorous

· In QC, we refer this more coz it's a complete molecule instead of base.

· Chain of bases ⇒ Sequence of nucleotides

· 23 chromosomes pairs.

· 3 billion pairs → decomposed to chromosomes [decomposed to] → Genes.

· In human body, genes are:
- → 20k for male
- → 23k for female

This is diff coz,
22 chromes → same
+ 1 chromosome is diff.

X(X) male — X(Y) Female

This adds a lot of genes than (X)

· Humans evolved from bacteria
- Hydra
- Amoeba
- Unicell

Very primitive

but humans have 27 trillion cells

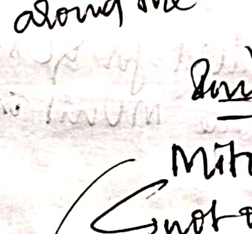
not well organised/well formed such cells are called Procaryote. → Cell is in early stage

fully formed/Evolved cell called Eucaryate.

· Our DNA is identical to an extent of 99.5% → all human race around the world.
↳ rest 0.5% diff coz of mutations.

Snp Characteristics

Mitochondria
↳ not only power house, also gives signature of motherlyness.
↳ has a DNA, so a child can be tracked easily from mother's lineage >>> father's lineage
- mother's lineage → mitochondria preserved
- father's lineage → fades out



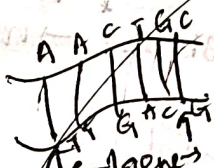
→ lineage of all mothers of mitochondria of all these species is same.

Protein Synthesis

- most imp regulatory function of the cell.
- for a human to survive we need
  - food (includes water also)
  - Oxygen
  - shld be eventually converted to energy
    - for this we need enzymes
      - a type of protein.
- Pituitary gland responsible for hormones.
- Pancreas → Synthesize insulin
  - means generate
  - converts sugar to energy
  - if ✗ blood will carry sugar.
- There are 20 diff types of hormones
  - growth & regulation
  - this also is proteins.

- Proteins
  - Enzymes
    - Eg: Saliva
    - generated in the cells of tissues at oral track & start digesting there itself.
  - Hormones
    - created at 1 place, transferred through blood to other place.
    - → used throughout the body.
- Generate there itself [Creation/Usage]

- For cell survival, we need 'O's & energy, transmitted by blood, to almost 3 trillion cells.
- Even if 1 cell → no 'O' → it dies.
- There a lot of computations that take place
- ~~[illegible]~~
- Instructions are generated from nucleolus.
- When a protein needs to be synthesized, it finds starting point & ending point in bp. The movement it decides to synthesize protein, the is to determined → How?

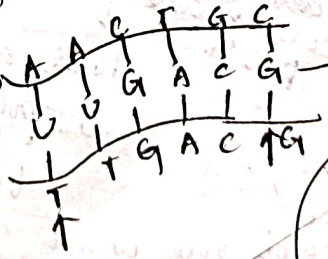


→ responsible for protein synthesis

- The 2 strands are separated within the cell nucleus (or) opened.

→ Involves 2 steps
1) Transcription
2) Translation.

- In 1) there is a process called mRNA. messenger is created
  - DNA → Deoxy Ribo Nucleic Acid
    - ATGC → molecules in DNA.
  - RNA → Ribo Nucleic Acid.
    - In RNA, we have AUGC (Uracil)

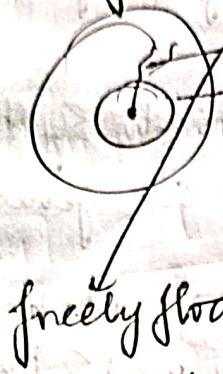


→ UUGACG (mRNA)

A–U
G–C
T–A
C–G

just thymine is replaced.

• One mRNA is generated, it comes out of nucleus pores.



freely floats in Cytoplasm

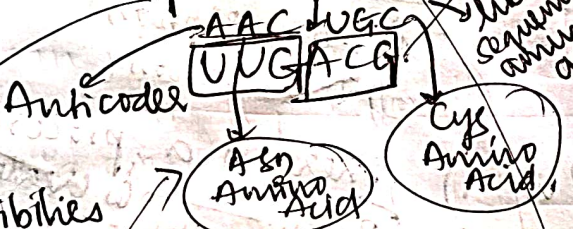
⇒ Here Transcription step is done.

⇒ Again, the strings are combined, i.e., After Transcription, original state is restored — no degradation

• Ribosome ← The bp is run through this

or

• Translation System is passed on this triplet code



possibilities

↳ 4 · 4 · 4 → 64 possibilities

↓ Can be manufactured

Again 64 Anticodon possibilities.

⇒ Diag

- quite many codes can code to same protein.

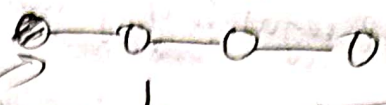
There are 64 possibly but only 20 Amino Acids.

3 Phe, Leu

↓ each one is an amino acid

• Central Dogma a refer to → see pic

• This process is Translation



↓ bonds are formed called peptide bond.

⇒ Every protein is identified by 1 begin & 1 stop.

⇒ AUG — Met → is start (Methionine → 1st amino acid for every p. synthesis)

UAA
UAG
UGA
} Stop → For every gene

⇒ This synthesized protein is passed through Quality check

↓ Sugar is responsible whether it is fabricated/not.

⇒ Then it is properly wrapped & transfered if its a hormone.

Utube → P sgs → Go through

Types

rRNA → Ribosome

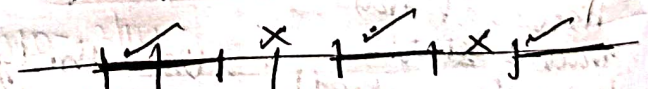
tRNA → transpts

mRNA → Non-coding DNA (throughout life it is in always dormant state)

⇒ Junk DNA → 98% of DNA

↓ 3 Billion bps

⇒ Suppose there are 1000 bps,



useful for transcription

Not useful for (Intermittent Junk DNA)

we combine only these 3 parts, by leaving all Junk DNA is passed through pores to cytoplasm. 2 imp [link

(1) Mitosis & Meiosis — protein synthesis, germ cells for reprodn system

25/02/24 — Unit-5

Quantum Error Correction:

EC → Detect & Rectify.

- Compared to Digital comm, Q commn is error prone becoz of every physical characteristics.
  - ↳ each one contributes some kind of error. Eg: Inference, coherence etc.
- We need to design EC techniques.
- Qubit cannot be cloned.
  - ↳ No cloning technique

① Brute Force [Repetition Code].

$|0\rangle \longrightarrow |000\rangle$

(Assumption)

- If Error occurrence is very rare, only 1 bit is corrupted.
- So, instead of 1 bit if we send 3 bits, we can see majority of 3.

DisAdv:

- B/w is ↑ by 3x

→ Quality is more important means we go for qualitative approach.

→ This is ... So, in those cases we use this.

→ Each code is repeated 3 times.

3 bit repetition codes

0 ⟼ 000

1 ⟼ 111

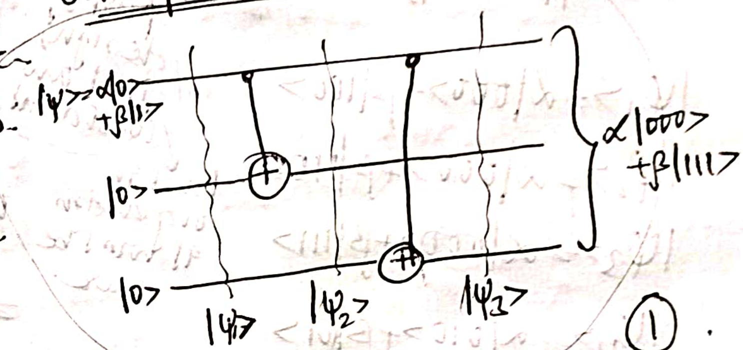
Decoding:

abc → majority (a,b,c) → o/p is corrected bit.

Eg: 001 → majority is 0, so 0 is corrupted.

- But this fails if we get majority 2 vals.
- In this, we use either 3/5 but we can't with even becoz of tie-breaking problem.

Corresponding Q. Circuit:



CNOT gate:

0	0	0
0	1	1
1	0	1
1	1	0

$|\psi_1\rangle = \alpha|000\rangle + \beta|100\rangle$

$|\psi_2\rangle = \alpha|000\rangle + \beta|110\rangle$ [CNOT on 1st & 2nd]

$|\psi_3\rangle = \alpha|000\rangle + \beta|111\rangle$ [CNOT on 1st & 3rd]

- Here $|\psi\rangle$ is not replicated only bits are replicated.
  - ↳ $|\psi\rangle|\psi\rangle|\psi\rangle$ → like $(a+b)^3$ — we are only considering $a^3 + b^3$ & ignoring rest. So, only bits.

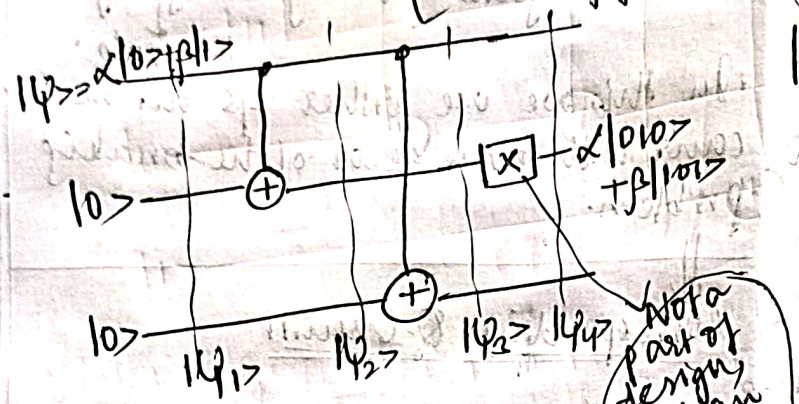
→ So, No cloning theorem.

require

• $|x\rangle$ → bit flip } Noise can be caused by any of these
• $|z\rangle$ → phase flip }

Bit flip correction

(See from prev diag for ref)



$|\psi_1\rangle = \alpha|000\rangle + \beta|100\rangle$

$|\psi_2\rangle = \alpha|000\rangle + \beta|110\rangle$

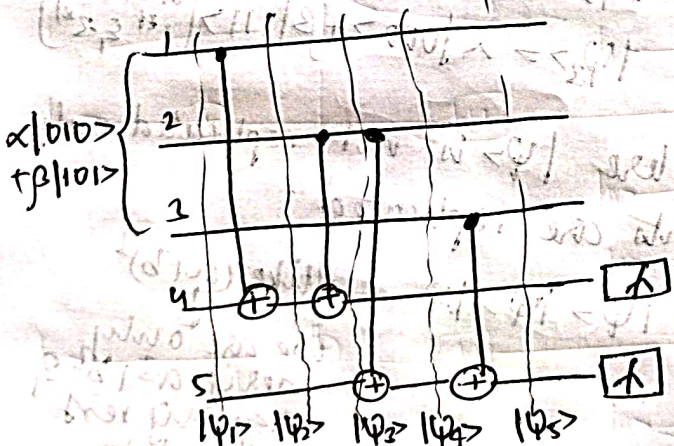
$|\psi_3\rangle = \alpha|000\rangle + \beta|111\rangle$

$|\psi_4\rangle = \alpha|010\rangle + \beta|101\rangle$

But in org design it won't be there

• We will write an another QC to see where exactly corruption is taking place

• We can identify the location of a single bit flip with the following circuit



• In the EC stage, we are taking the help of 2 more Qubits.

∴ This is a circuit of 5 Qubits.

• This is so expensive because it is not reliable with 1 Qubit.

∴ So this 5 bit QC.

⇒ A → this is very imp.

This is what for bit flip

∴ this decides which bit is corrupted.

$|\psi_1\rangle = \alpha|01000\rangle + \beta|10100\rangle$

$|\psi_2\rangle = \alpha|01000\rangle + \beta|10110\rangle$

$|\psi_2\rangle = \alpha|01010\rangle + \beta|10110\rangle$

$|\psi_4\rangle = \alpha|01011\rangle + \beta|10110\rangle$

$|\psi_5\rangle = \alpha|01011\rangle + \beta|10111\rangle$

4th & 5th → are considered.

⇒ last 2 are 1 1.

The Q.C is designed such that there is sym b/w 4th & 5th bit — =

i.e, α & β → 4, 5 bits are same

1 A 1 A

1 1 → Middle bit is corrupted.

0 0 → No bit is corrupted

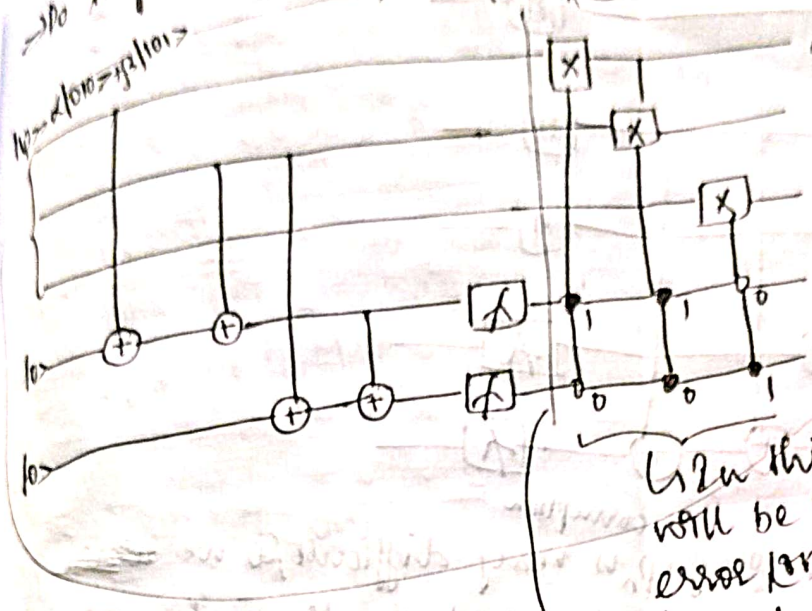
State	Syndrome	Correction
$\alpha\|000\rangle + \beta\|111\rangle$	0 0	$1 \otimes 1 \otimes 1$
$\alpha\|100\rangle + \beta\|011\rangle$	1 0	$X \otimes 1 \otimes 1$
$\alpha\|010\rangle + \beta\|101\rangle$	1 1	$1 \otimes X \otimes 1$
$\alpha\|001\rangle + \beta\|110\rangle$	0 1	$1 \otimes 1 \otimes X$.

1 → unaltered
X → flipped

Cont...

→ Do 91 for 1st & 2nd bit also.

↳ corruption in |x⟩.

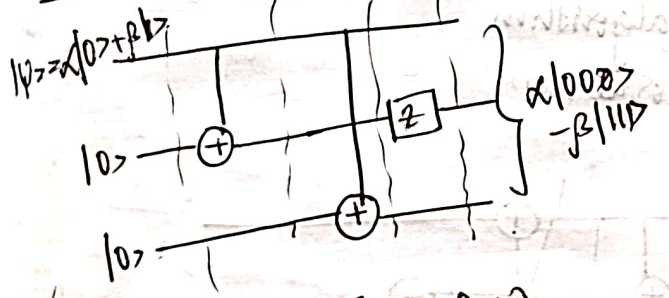


① ↳ In this any one of the these will be invoked, if there is any error else our logic can be stopped → here

→ ① + ③ → complete diagram. Combine them for complete circuit → Q. Correction is very expensive that's why.

⇒ Phase flip

This is to explain why prev circuit should not be used.



$|\psi_1\rangle = \alpha|000\rangle + \beta|100\rangle$

$|\psi_2\rangle = \alpha|000\rangle + \beta|110\rangle$

$|\psi_3\rangle = \alpha|000\rangle + \beta|111\rangle$

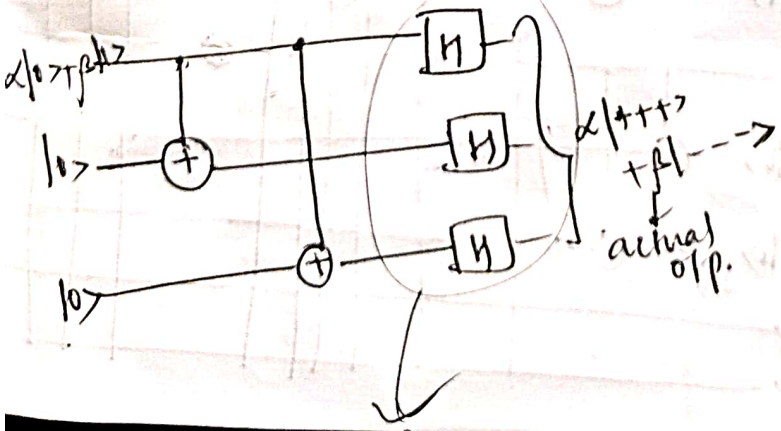
$|\psi_4\rangle = \alpha|000\rangle - \beta|111\rangle$

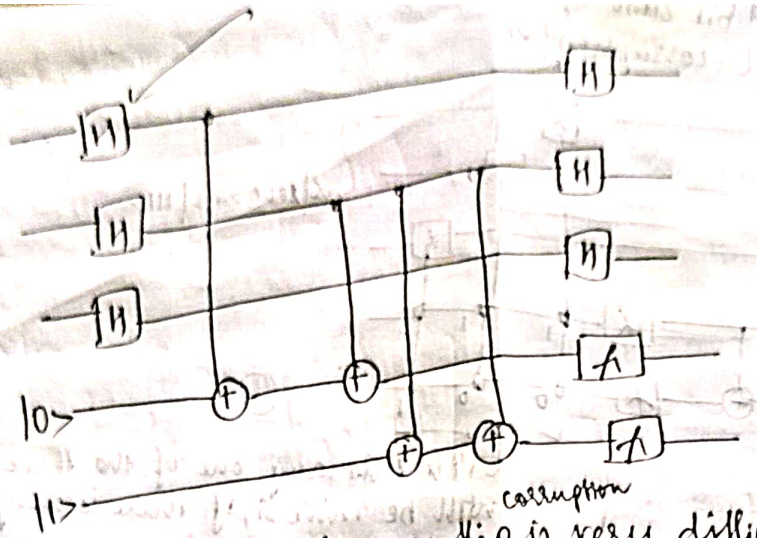
↳ Here no bit is changing so prev circuit not suitable, so we are adding H gates.

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

↳ modified to.

actual circuit





• Identifying bit flip & phase flip corruption is very difficult, so we try to draw a diff Q.C. to tackle both flips at a time, as we cannot do separately.

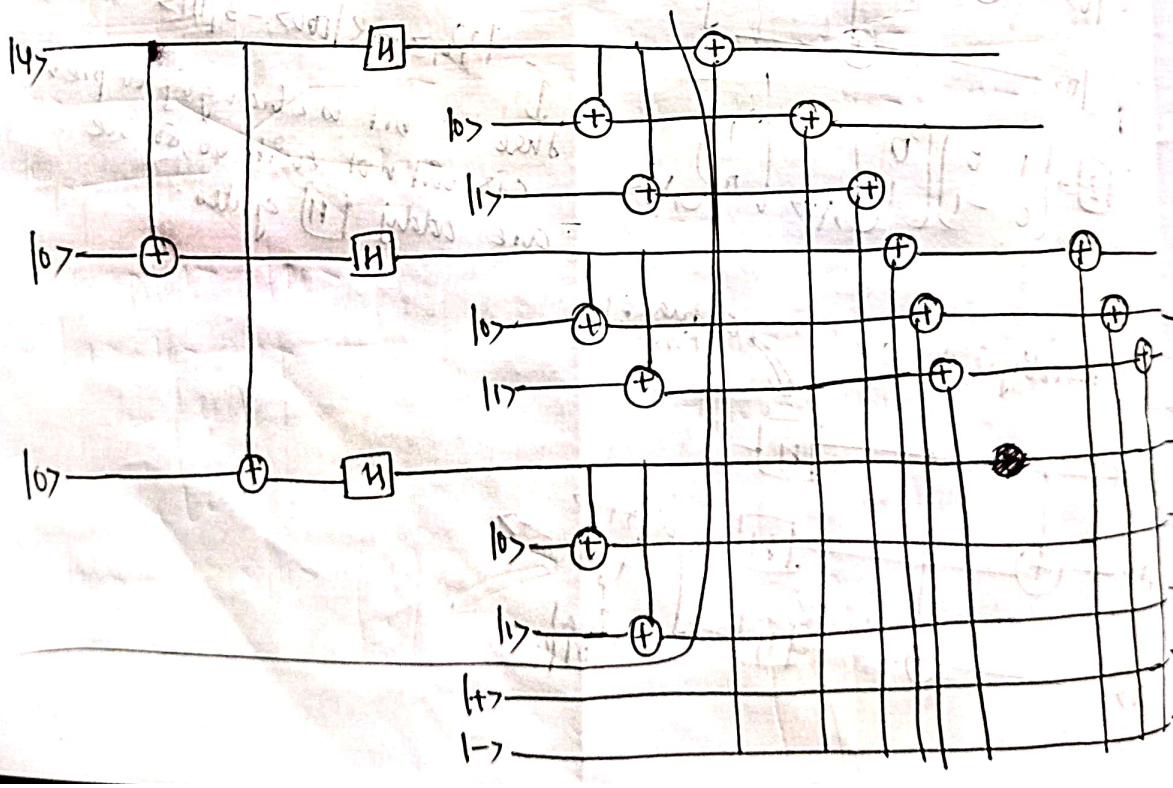
• Both flips use 5 bits for detection, but for both now we are using 9 bits.

↓

known as 9 bit shore code (to tackle both bit flip & phase flip)

↓

very famous algorithm in Q.C correction.



• Unitary matrix — $UU^\dagger =$

• Hermitian matrix → $U^\dagger =$

A matrix which is u
not be hermitian & vice-

→ $U = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $U^\dagger =$

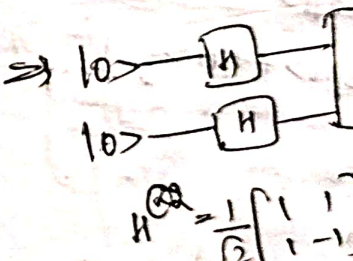
→ Entire quantum cir
represented as a single
↳ Emp

If there are n qubits

$\Rightarrow A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot B =$

$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix}$

$= \begin{bmatrix} a_{11}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21}\begin{bmatrix} \quad \end{bmatrix} \end{bmatrix}$



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

$= \frac{1}{2}$

ASSIGNMENT QXI

1. Unitary matrix — $UU^\dagger = U^\dagger U = I$
2. Hermitian matrix $\hookrightarrow U^\dagger = U$

→ matrix which is unitary might not be hermitian & vice-versa.

$$U = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad U^\dagger = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

→ Entire quantum circuit can be represented as a single unitary matrix
↳ Imp.

If there are n qubits ⇒ matrix dimension ↓ $2^n \times 2^n$.

⇒ $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$

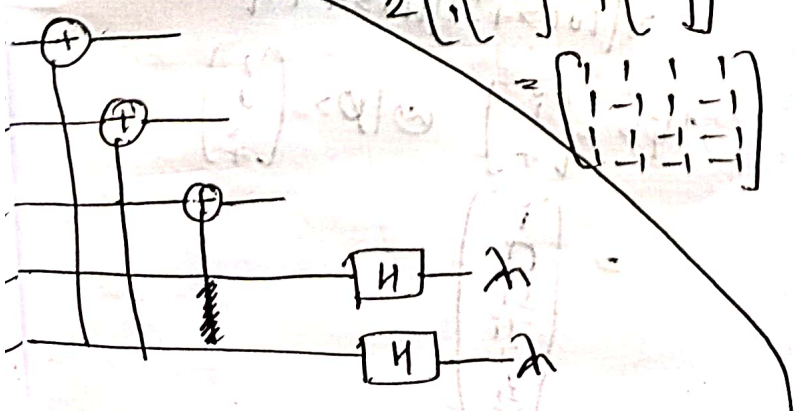
$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix} = \begin{bmatrix} a_{11}\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12}[\ ] \\ a_{21}[\ \ ] & a_{22}[\ ] \end{bmatrix}_{4\times4}$$

⇒ |0> — H
|0> — H

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

$$= \frac{1}{2}\begin{bmatrix} 1[\ ] & 1[\ ] \\ 1[\ ] & 1[\ ] \end{bmatrix}$$

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



- All single Qubits are represented as 2×2 matrix.
- 2 Qubits → 4×4 → dimensionality depends on gates

C-NOT	
Input	Output
00	00
01	01
10	11
11	10

C-NOT Unitary Matrix

$$\begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array}\begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times4} \end{array}$$

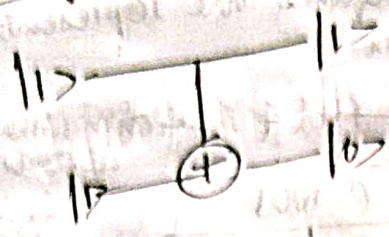
C-CNOT gate / controlled

1's → flip

Input	Output
000	000
001	001
010	010
011	011
100	100
101	101
110	111
111	110

$$\begin{array}{c} \\ 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{array}\begin{array}{c} \begin{array}{cccccccc} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}_{8\times8} \end{array}$$

CNOT gate



$$\Rightarrow |1\rangle \otimes |1\rangle$$

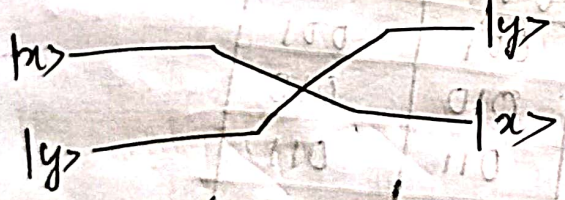
$$\begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\begin{bmatrix}0\\1\end{bmatrix}\\1\begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

⇒ For tensor products all the qb's are column matrix.

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

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

Swap gate



Swap $|01\rangle = |10\rangle$

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

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

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

Controlled Hadamard Gate

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

→ is replaced with [H] gate for controlled

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

$$|a\rangle|b\rangle = [\ ] \otimes [\ ]$$ [ker-ker]

→ convert Q-states to matrix form first.

① $|\psi\rangle = 9|0\rangle + 7|1\rangle \rightarrow [\ ]_{2\times 1}$

$|\psi\rangle = |00\rangle + 3|10\rangle + 7|11\rangle \rightarrow [\ ]_{4\times 1}$

$|\psi\psi\rangle = [\ ]_{8\times 1}$

$= 9|000\rangle + 3i|010\rangle + 7i|011\rangle + 7|100\rangle + 21|110\rangle + 49|111\rangle$

$$|\psi\rangle = \begin{bmatrix}9\\7\end{bmatrix} \otimes |\phi\rangle = \begin{bmatrix}1\\0\\3\\7\end{bmatrix}$$

$$= \begin{bmatrix}9\\0\\3i\\7i\\7\\21\\49\end{bmatrix}$$

4.

③ Bra is not represented as horizontal (row matrix)
↳ rest computations are identical to prev Q.
→ won't be there.

⑥ Ket - Ket

④ Take 1st 2 terms → coz 1st & 4th are zeroes
↓
cal. prob. of each terms → usually 1st normalized but here already 1.

⑪ Ket - bra
↳ Not product of tensor prod
↳ $|\alpha\rangle\langle\beta|$

$|\alpha\rangle = 3|0\rangle + i|1\rangle$

$|\beta\rangle = |00\rangle + 2|10\rangle + 7|11\rangle$

$\langle\beta| = \langle 00| + 2\langle 10| + 7\langle 11|$

$|\alpha\rangle\langle\beta| = 3|0\rangle\langle 00| + 6|0\rangle\langle 10| + 21|0\rangle\langle 11| + i|1\rangle\langle 00| + 2i|1\rangle\langle 10| + 7i|1\rangle\langle 11|$

	00	01	10	11
0	3	0	6	21
1	i	0	2i	7i

⑧ Compute the norm

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

⑨ $\langle +|-\rangle \Rightarrow 0$ → orthonormal (1 log)

⑩ Use Hint.
↳ dont use matrix, show in expression form
↳ & square the coefficients should be equal to 1
↳ show that.

⑪ $\langle\psi|0\rangle$

⑫ $e^{i\theta} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$

$= \cos\pi/2 + i\sin\pi/2 = i$

$i|\psi\rangle = i\left(\frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\right)$

$= 9|+\rangle$

⑫ Solved in prev page

⑭ Use CNOT matrix.
① easy peasy
②
↓
next page

⇒ Norm of $|\alpha\rangle$
↳ (Bra-ket)
↳ $\sqrt{\langle\alpha|\alpha\rangle} = 1$ → means unit vector
↓
means q.state is normalised.

$\langle 0|0\rangle$

⑤ ~~Ket - bra~~

$\langle\alpha| = -i\langle 0| + 7\langle 1|$

$|\beta\rangle = |\beta\rangle$.

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

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

CNOT $|+\rangle$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

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

$$\Downarrow$$

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

---

(15) R_{90} → rotation gate.

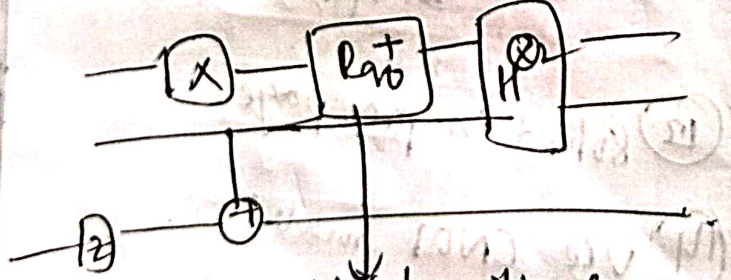
(a) can be reversed only when all the gates used are hermitian

hdirectly

~~b[illegible]~~

left = right

Here, only R_{90} is not hermitian.

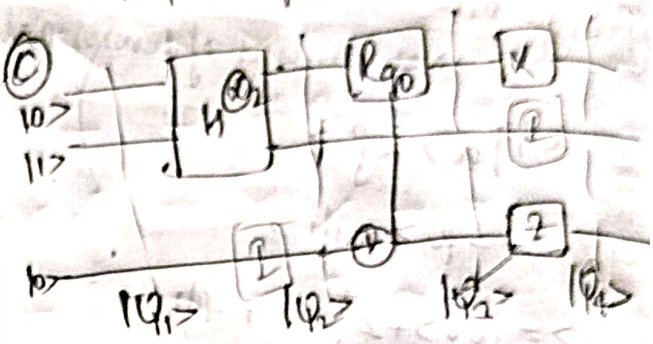


(b) $R_{90}|0\rangle \rightarrow \begin{bmatrix} \cos 90 & -\sin 90 \\ \sin 90 & \cos 90 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

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

$R_{90}|1\rangle = |0\rangle$

(c)



Stage 1:

$H \otimes H \otimes I$ (2×2) (2×2) (2×2) → 8×8

S_2 : $R_0 \times CNOT \Rightarrow 8\times 8$

2×2 4×4 → $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$S_3 = X \otimes I \otimes Z \Rightarrow 8\times 8$.

$S_1 \times S_2 \times S_3$ → not correct

$S_3 \times S_2 \times S_1$ → correct order.

multiplied

↳ scalar product.

Every QC can be represented as Unitary Matrix

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}_{8\times 1}$$

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

$$\begin{bmatrix} \cdot & \cdot \\ \cdot & \cdot \end{bmatrix}_{8\times 8} \otimes \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}$$

$$\Downarrow$$

$$\begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{bmatrix}_{8\times 1}$$

24/08/25 ① Diffe- ③ RSA
· ECC, Hellmann, etc.

↳ Assymetric key security.

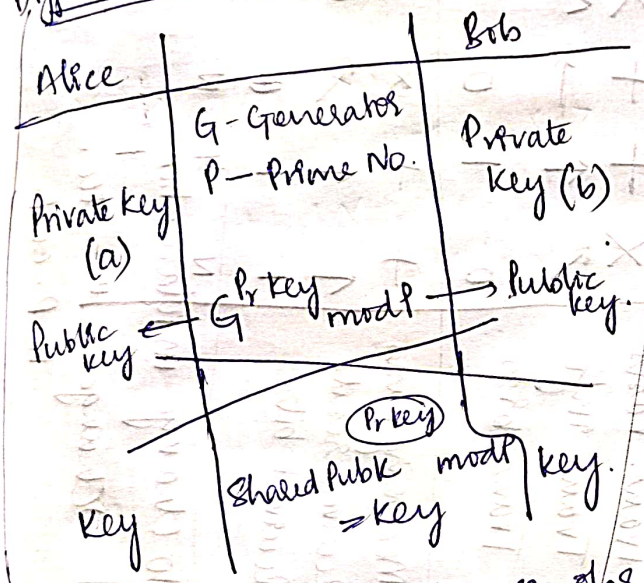
↓

Pu is shared, Pr is X.

→ $(P)_c$ & $(P)_c$ → diff.

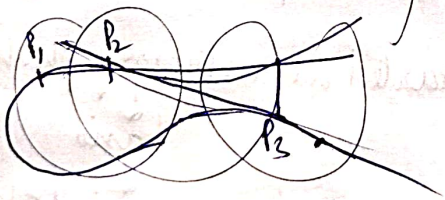
→ Another implementation is there where both parties share same key for E & D, but this key is not shared through channel, they generate on their own but same key.

Diffie Hellmann Alg → most successful & acceptable encryption algm



↳ we are following this similar approach in Q. Cryptography.

ECC:



$$\begin{cases} y^2 = x^3 + ax + b \\ 4a^3 + 27b^2 \bmod P \neq 0 \end{cases}$$

↳ Variable → (a, b, P)

with this by chay, we can make ∞ curves.

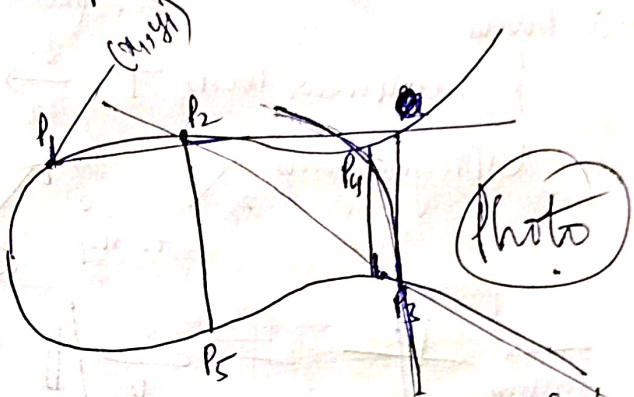
· Some maybe bulged, small

↳ symmetric property is remained.

Ex:
1 $P_1 + P_2 = P_3$
2 $P_1 + P_3 = P_4$
3 $P_4 + P_4 = P_6$

P → points.

→ This is constructed such as when we are joining 2 points, if we extend that line, we find a 3rd point on ellipse.



After 'n' operations we get a point (x_1, y_1) on the surface of the curve that is used as a key in the cryptography process.

Initially a, b, P_1, P_2 & n are given the last point is calculated using these ① + ② + ③ ∴ imp ✗✗

Q. Cryptography

· Key Generation is difficult.

· Photons are perceived as particles

↳ has polarization.

↳ we can change the alignment

↓

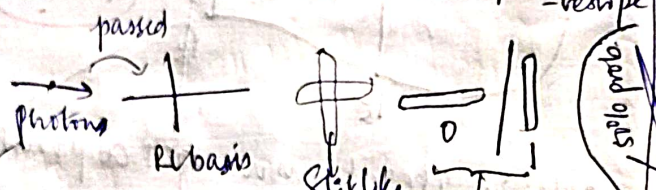
+ve, -ve slope

· Stream of photons passed through laser / basis, [See Next Page]

Quantum Key Distribution

- QK is used in QC
- Polarization of photons is a quantum mechanics property. (particle nor wave)
- Photons by default, which are in superposn state collapses to one of the states, when passed through the basis.
  (quantum)

→ 2 basis
  → Rectilinear basis + → horizontal polarization
    0 ↑ 1
  → Diagnol basis ×
    ↖ 0 +veslope
    ↗ 1 -veslope



- Photon which is in ~~polarised~~ state, shld select which polarisation it shld use.
- Photons won't be divided, initially 1000 means final also 1000.

can be either one of this

→ Similarly

can be any one of these 4. position vectors.

Transmission end (Alice)	Trans. basis	+	+	×	×	+	×	+	+	×	×	+	×	×	+	+	×	×	+
	Trans. info	↑	←	↗	↖	↑	↖	↑	↑	↖	↙	←	↙	↙	←	↑	↖	↙	←
	Trans. bits	0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0	1	1
Receiving end (Bob)	Measuring basis	+	×	×	×	+	×	+	+	×	×	+	×	×	+	+	×	×	+
	Received result	↑	↗	↖	↖	↑	↖	↑	↑	↖	↙	←	↙	↙	←	↑	↖	↙	←
	Received bits	0	1	1	0	0	0	0	0	0	1	1	1	1	1	0	0	1	1
% Tr = Rec, NO change in Polarization		N	N	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	Y	Y	Y	N	Y
Trans + Rec → Change		Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Key = 1101 01

We started at arbitrary photons
↓
basis
↓
polarised state
↓
bits

- Alice to Bob → photon sharing is done which might change but basis shld be same

BB84 protocol