→ QFT
→ Equation (Definition)
→ Application
→ Advantages → efficient, scalable.
$O(n^2)$ over $O(n2^n)$

STUDENT'S NAME | TOTAL MARKS OBTAINED
CLASS | SUBJECT
DATE

Quantum Fourier Transform

Time domain ——————→ Frequency domain

Hadamard gate [converts <01 or 1-> to superposition state]
↓
Controlled Phase gates [Introduces Phase shifts to the Qubits] [Rotation varaund Z-axis]
↓
Swap gates [Order of qubits may be reversed to toget desired output]

Application → Phase estimation
→ Order finding problem & factorial problem
→ Counting problems/solutions
→ Hidden subgroup problem

Apply fourier transform on 1qubit, 2Qubit, 3Qubit
Input Vector complex —transformed data→ Vector Complex no
no length-N

$|0\rangle$ & $|1\rangle$ $\qquad$ $|+\rangle$ & $|-\rangle$

Vector representation $\begin{bmatrix}1\\0\end{bmatrix}$ $\begin{bmatrix}0\\1\end{bmatrix}$ $\qquad$ $\frac{1}{2}\begin{bmatrix}1\\1\end{bmatrix}$ & $\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$

Integral Transform

$\{x\} \xrightarrow[IT]{} \{y\}$

kernel

$$IT\{x\} = K(x,y)\{y\}$$

(1) $$QFT|x\rangle = K(x,y)|y\rangle$$

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

function of input as well as output

$$\rightarrow \sqrt[N]{1} = \omega_N = e^{\frac{2\pi i}{N}}$$

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N} \omega_N^{xy} |y\rangle$$

EBSONS

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i xy}{N}} |y\rangle$$

for 1 qubit i.e $N = 2^n \Rightarrow 2^n = 2^1 \Rightarrow N = 2 \Rightarrow$ **$y = 0$ & $y = 1$**

$$QFT|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\frac{2\pi i xy}{2}} |y\rangle$$

x & y are decimal
$x \cdot y$ = Multiplication

Substitute $y = 0$ & $y = 1$

for coherence $\rightarrow |\tilde{x}\rangle = \frac{1}{\sqrt{2}} \left[e^{\frac{2\pi i x(0)}{2}} + e^{\frac{2\pi i x(1)}{2}} \right]$

Now

$$= \frac{1}{\sqrt{2}} \left[e^{\frac{2\pi i x}{2}} |0\rangle + e^{\frac{2\pi i x}{2}} |1\rangle \right]$$

Substitute for $x = 0$ & $x = 1$

$$\frac{1}{\sqrt{2}} [|0\rangle + |1\rangle] \qquad \frac{1}{\sqrt{2}} [|0\rangle - |1\rangle]$$

$$|+\rangle \qquad |-\rangle$$

for $|\tilde{0}\rangle = |+\rangle$ & for $|\tilde{1}\rangle = |-\rangle$

for linear equation

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

$\downarrow$ QFT

$QFT|\psi\rangle = \alpha|\tilde{0}\rangle + \beta|\tilde{1}\rangle$

$= \alpha[|\tilde{+}\rangle + |\tilde{-}\rangle]$

$= \alpha\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] + \beta\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$

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

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

What is y.

$$QFT\,|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle \quad \cdots (1)$$

$y = y_1, y_2, y_3 \cdots y_n$ (only 0 to 1) Binary

Decimal ← Binary

(2) $= y_1 2^{n-1} + y_2 \times 2^{n-2} + y_3 \times 2^{n-3} \cdots + y_{n-1} \cdot 2^1 + \underbrace{y_n}_{y_n 2^0} 2^{n-0}$

$$\therefore \boxed{y = \sum_{k=1}^{n} y_k 2^{n-k}} \quad \cdots (2)$$

Substitute equation (2) in equ (1) for y

$$QFT|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x \sum_{y=1}^{N} y_n 2^{n-k}}{N}} |y_1 y_2 y_3 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x \sum_{k=1}^{N} y_k 2^{n-k}}{2^n}} |y_1, y_2, y_3 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x \sum_{y=1}^{N} y_k 2^n \cdot 2^{-k}}{2^n}} |y_1, y_2, y_3 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x \sum_{y=1}^{N} \frac{y_k}{2^k}} \langle y_1, y_2, y_3 \cdots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2\pi i x y_k}{2^k}} |y_1, y_2, y_3 \cdots y_n\rangle$$

$e^{x+y+z} = e^x \cdot e^y \cdot e^z$

$e^{\sum x_i} = \prod_i e^{x_i}$

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2\pi i x y_k}{2^k}} |y_1 y_2 \cdots y_n\rangle$$

y_k

$$\hookrightarrow \left[\sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \sum_{y_3=0}^{1} \cdots \sum_{y_n=0}^{1} \right]$$

$$= \frac{1}{\sqrt{N}} \prod_{k=1}^{n} \left[\sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \sum_{y_3=0}^{1} \cdots \sum_{y_n=0}^{1} e^{\frac{2\pi i x y_k}{2^k}} |y_k\rangle \right] \quad y_k \to 0,1$$

Tensor product

$$= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} \left[|0\rangle + e^{\frac{2\pi i x y}{2^k}} \right]$$

Now substitute for k=1 to n as tensor product

$$= \frac{1}{\sqrt{N}} \left[|0\rangle + e^{\frac{2\pi i x}{2^1}} \right] \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^2}} \right] \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^3}} \right] \cdots \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^n}} \right]$$

NEXT

- $x_1 x_2 x_3$ in equation

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

Quantum Fourier Transform:-

Circuit for QFT: $|X\rangle = \frac{1}{\sqrt{N}}\left[|0\rangle + e^{\frac{2\pi i x}{2}}|1\rangle\right] \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^2}}|1\rangle\right)$ (phase change)

$\otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^n}}|1\rangle\right]$ (phase change, nth Qbit)

first Qbit — 2nd Qbit

Tensor product of X. ⇧ Output

Why tensor product in the circuit

First Qbit should become → Transformation

1) $\longrightarrow \left(|0\rangle + e^{\frac{2\pi i x}{2}}|1\rangle\right)$

↓

Hadmard gate. [First Qbit Hadmard will be operated]

(1) $|x\rangle$ — H — $= \left(|0\rangle + e^{\frac{2\pi i x}{2}}|1\rangle\right)$

(2) Phase of $|0\rangle$ remains same but for $|1\rangle$ phase is $e^{\frac{2\pi i x}{2^2}}$

for n^{th} bit phase $e^{\frac{2\pi i x}{2^n}}$

Rotational operator U_{Rot}

U_{Rot}^n — $|0\rangle$ (ket-0) → no change

$|1\rangle$ (ket-1) → $e^{\frac{2\pi i}{2^n}}$ (operating on n^{th} qubit)

Example → $|x_1\rangle$ — H — U_{Rot}^2

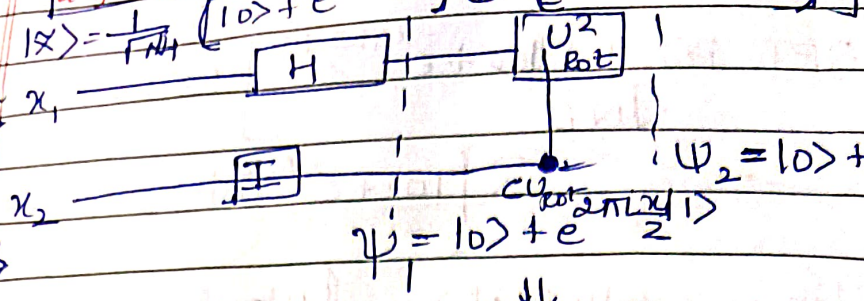
$|x_2\rangle$ — (reverse)

$U_{Rot}^n = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^n}} \end{bmatrix}$ → matrix should be

Practice

2 Qubits : $2^2 = 4$

$|x\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle + e^{2\pi i \frac{x_1}{2}}\right) \circledast \left[|0\rangle + e^{2\pi i \frac{x_2}{2^2}}\right]$



$\Rightarrow H \circledast I \; |x_1 x_2|$

$H|x_1\rangle \circledast |x_2\rangle$

$|0\rangle + e^{2\pi i \frac{x_1}{2}}|1\rangle \circledast |x_2\rangle \Rightarrow |0\rangle + e^{2\pi i \frac{x_1}{2}}|1\rangle \circledast U^2_{Rot} \cdot |x_2\rangle$

Write again =

$U^n|x\rangle = |0\rangle + e^{\frac{2\pi i x}{2^n}}|1\rangle$

$\boxed{U^2|x_2\rangle = |0\rangle + e^{\frac{2\pi i x_2}{2^2}}|1\rangle}$

$\psi_2 \Rightarrow \left(|0\rangle + e^{2\pi i \frac{x_1}{2}}\right) \circledast \left(|0\rangle + e^{2\pi i \frac{x_2}{2^2}}|1\rangle\right)$

$\Rightarrow \left(|0\rangle + e^{2\pi i \left(\frac{x_1}{2} + \frac{x_2}{2^2}\right)}|1\rangle\right)$

$\Rightarrow \left(|0\rangle + e^{2\pi i (0.x_1 + 0.0x_2)}\right.$

$\psi_2 \Rightarrow \left(|0\rangle + e^{2\pi i (0.x_1 x_2)}|1\rangle\right)$

~~$\Rightarrow |0\rangle + e^{2\pi i}$~~

$\psi_f = \left(|0\rangle + e^{2\pi i (0.x_1 x_2)}|1\rangle\right)\left(|0\rangle + e^{2\pi i (0.x_1)}|1\rangle\right)$ from circuit

$\psi_f =$

$QFT(x_1 x_2) = \frac{1}{\sqrt{4}}\left[|0\rangle + e^{2\pi i (0.x_2)}|1\rangle\right) \circledast \left(|0\rangle + e^{2\pi i (0.x_1 x_2)}|1\rangle\right)$

STUDENT'S NAME		TOTAL M OBTAIN
CLASS	SUBJECT	
ROLL NO.	DATE	

$$QFT|x\rangle = \frac{1}{\sqrt{N}}\left[|0\rangle + e^{2\pi i \frac{x}{2}}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \frac{x}{2^2}}|1\rangle\right) \otimes \cdots \left(|0\rangle + e^{2\pi i \frac{x}{2^n}}|1\rangle\right)$$

Now consider $\frac{x}{2^n} = \frac{x_1 x_2 x_3 \cdots x_{n-1} x_n}{2^n}$

(3)

$$= \frac{1}{2^n}\left[x_1 x_2 x_3 \cdots x_{n-1} x_n\right]$$

$$= \frac{1}{2^n}\left[x_1 * 2^{n-1} + x_2 2^{n-2} + \cdots x_{n-1} * 2^1 + x_n \times 2^0\right]$$

Binary fraction

$$\frac{x}{2^n} = \frac{x_1}{2} + \frac{x_2}{2^2} + \frac{x^3}{2^3} \cdots + \frac{x^n}{2^n}$$

Now consider 3 Qubits

$$5 = \underset{2^2 2^1 2^0}{101}$$

$$= 1*2^2 + 0*2^1 + 1*2^0$$

$$5 = 4 + 0 + 1$$

Now Decimal to binary

$$\frac{123}{10^2} = 1.23 \Rightarrow \frac{x_1 x_2 x_3}{2^2} \Rightarrow x_1 . x_2 x_3$$

Ex: $\frac{5}{2^n} = \frac{5}{2^3} \Rightarrow 0.101$

$= \frac{5}{2^2} = 0.01$

$= \frac{5}{2} = 0.1$

$\frac{7}{2^n} = 111$

$\frac{7}{2^3} = 0.111$

$\frac{7}{2^2} = 0.11$

$\frac{7}{2} = 0.1$

ie $e^{2\pi i \frac{x}{2}} \Rightarrow e^{2\pi i \frac{5}{2}} \Rightarrow e^{2\pi i 0.1}$

$\Rightarrow e^{2\pi 5/2^3} \Rightarrow e^{2\pi i 0.101}$

$$\Rightarrow \therefore \frac{x}{2^3} = 0.x_{n-2}\, x_{n-1}\, x_n$$

$$\frac{x}{2^2} = 0.x_{n-1}\, x_n$$

$$\frac{x}{2} = 0.x_n$$

$$\frac{x}{2^n} = 0.x_1 x_2 \cdots x_n$$

$$\therefore \frac{1}{\sqrt{N}}\left[|0\rangle + e^{2\pi i(0.x_n)}|1\rangle\right] \otimes \left[|0\rangle + e^{2\pi i(0.x_{n-1}x_n)}|1\rangle\right)$$

$$\cdots \otimes \frac{1}{\sqrt{N}}\left[|0\rangle + e^{2\pi i(0.x_1 x_2 x_3 \cdots x_n)}|1\rangle\right)$$

Example:- 3 Qubits x_1, x_2, x_3

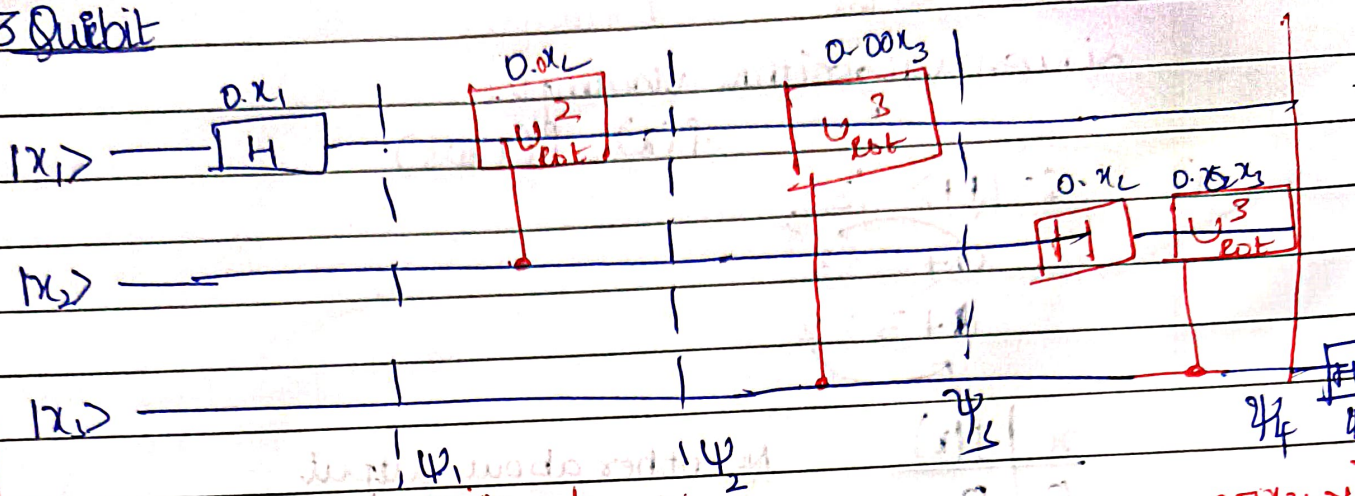
$$N = 2^3 = 8$$

$$= \frac{1}{8}\left[|0\rangle + e^{\frac{2\pi i x}{2}}|1\rangle\right] \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^2}}|1\rangle\right] \otimes \left[|0\rangle + e^{\frac{2\pi i x}{2^3}}|1\rangle\right]$$

$$= \frac{1}{8}\left[|0\rangle + e^{2\pi i 0.x_3}\right] \otimes \left[|0\rangle + e^{2\pi i 0.x_2 x_3}\right] \otimes \left[|0\rangle + e^{2\pi i 0.x_1 x_2 x_3}|1\rangle\right]$$

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

3 Qubit



practice

$|0\rangle + e^{2\pi i \frac{x_1}{2}}|1\rangle \; |x_2 x_3\rangle$

$\psi_2 = |0\rangle + e^{2\pi i \frac{x_1}{2}}|1\rangle) \otimes (|0\rangle + e^{2\pi i \frac{x_2}{2^2}}|1\rangle$

$$\psi_1 = \left(|0\rangle + e^{2\pi i \frac{x_1}{2}}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i \frac{x_2}{2^2}}|1\rangle\right) |x_3\rangle$$

$$\psi_2 = |0\rangle + e^{2\pi i \frac{x_1}{2}}|1\rangle) \otimes (|0\rangle + e^{2\pi i \frac{x_2}{2^2}}|1\rangle \otimes \left(|0\rangle + e^{2\pi i \frac{x_3}{2^3}}|1\rangle\right)$$

$\psi_3 = |0\rangle + e^{2\pi i (0.x_1 x_2 x_3)}|1\rangle$ → last term

$\psi_4 = |0\rangle + e^{2\pi i 0.x_2 x_3}|1\rangle$ → 2nd term

$\psi_5 = |0\rangle + e^{2\pi i (0.x_3)}|1\rangle$ → 1st term.

Step up

$$QFT|x_1 x_2\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle + e^{2\pi i (0.x_2)}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i (0.x_1 x_2)}|1\rangle\right.$$

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

SIMON'S Algorithm

→ Simon's algorithm in Quantum computing is a hybrid quantum classical algorithm designed to solve a specific problem exponentially faster than any classical algorithm.

→ The problem involves finding a hidden binary string s associated with a function f from n-bit strings to n-bit strings, where $f(x) = f(y)$ if and only if $y = x \oplus s$.

→ Goal:- Determine secret string

1. ~~Proof~~ Detailed derivation

Problem setup:- Given a function $f: \{0,1\}^n \to \{0,1\}^n$ with the promise that there is a secret string

① $s \in \{0,1\}^n$ such that

$$f(x) = f(y) \iff y = x \oplus s \quad \rightarrow \quad s = 0^n$$

one to one or two to one

→ XOR

2) Quantum circuit initialization-

Initialize 2n bit registers to the state:-

$$|0\rangle^{\otimes n} |0\rangle^{\otimes n}$$

3) Apply Hadamard Transform to first register. This generates an equal superposition of all n-bit strings

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n - 1} |x\rangle |0\rangle.$$

4) Oracle Query (unitary U_f): Apply the quantum oracle representation U_f.

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

resulting in

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

EBSONS

5) Measure the second Register.
Measure the second register. This collapses the state into a superposition of the inputs that map to the observed value $f(x_0)$:
$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle)\,|f(x_0)\rangle.$$
Ignore 2nd register as it is measured.

5)(b) Measure the second register.
Measurement collapses the second register to some value $f(x_0)$ and first register collapses into a superposition of $|x_0\rangle$ and $|x_0 \oplus s\rangle$:
$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus s\rangle).$$

6) Apply Hadamard Transform to first register.
The Hadamard transforms each qubit giving
$$\frac{1}{\sqrt{2}} \sum_{z \in \{0,1\}^n} \left[(-1)^{x_0 \cdot z} + (-1)^{(x_0 \oplus s)\cdot z} \right] |x\rangle,$$
where $x_0 \cdot z$ is the bitwise inner product modulo.

7) Simplify the expression.
$$(-1)^{(x_0 \oplus s)\cdot z} = (-1)^{x_0 \cdot z}(-1)^{s \cdot z}$$
Thus the amplitude for $|z\rangle$ becomes
$$\frac{1}{\sqrt{2}}(-1)^{x_0 \cdot z}(1 + (-1)^{s \cdot z}).$$

→ If $s \cdot z = 1 \pmod 2$, the amplitude is 0
→ If $s \cdot z = 0 \pmod 2$, the amplitude is non zero

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

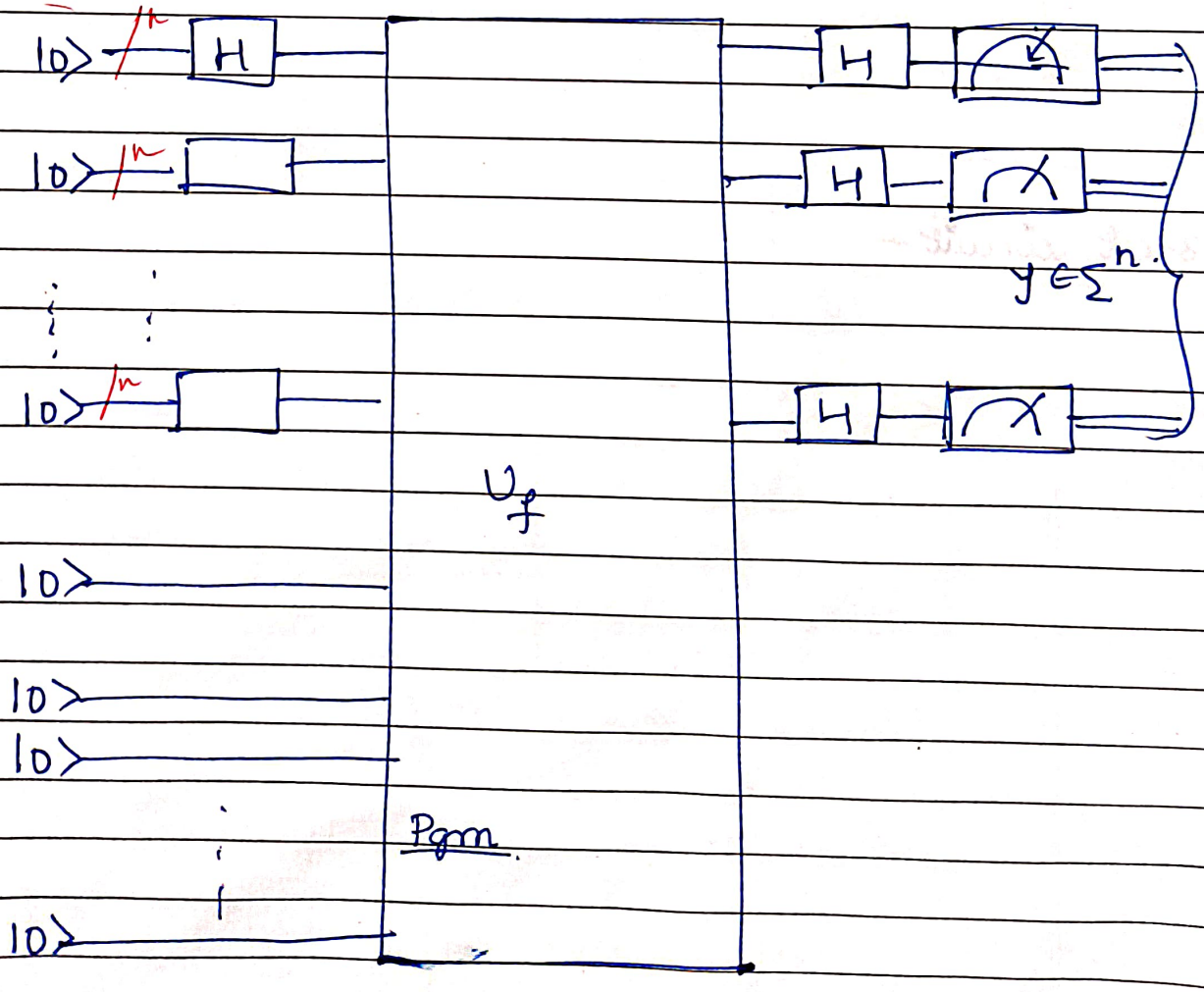
Circuit.

8) Measurement of First register: Measurement results only yield z such that:

$$s \cdot z = 0 \pmod 2$$

9) Classical post processing. Repeat steps 2-8 $O(n)$ times to collect enough linearly independant z's. Each satisfies $s \cdot z = 0$. Solve the system of linear equations modulo 2 to find the hidden string s.

Circuit.



→ Explaination of the circuit
→ Circuit for 2 bit
→ 3 bit
→ 4 bit

Pgm to run on system.

Medium

2bit circuit

3-bit circuit –

STUDENT'S NAME		TOTAL & OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

Simon Algorithm Example

2 qubit example.

$f(x) = f(x+s)$

a) $s = |11\rangle = |3\rangle_2$

Input

$x \Rightarrow$

$x+s \Rightarrow$ } same o/p

$s = 3$

$2^1 2^0 = 3$

$\Rightarrow$ 11

$\rightarrow$ $0 \oplus 3 = 3 \Rightarrow$ 0 & 3 same output | $(0+0) \oplus (2+1) = 3$

$1 \oplus 3 = 2 \Rightarrow$ 1 & 3 same output | $(0+1) \oplus (2+1) = 2$

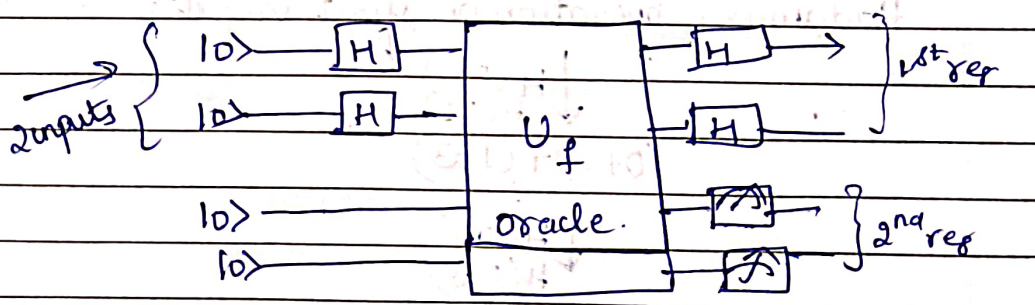
(2) $\Rightarrow$

x	f(x)
0	a
1	b
2	b
3	a

$\rightarrow$ Tabular ~~form for~~ corresponding to hidden Variable $s = 3$

$\Rightarrow$ Construct Quantum circuit

(3) Ex:-



$|x\rangle_2 |0\rangle_2 \xrightarrow{U_f} |x\rangle |f(x)\rangle$

output

x takes 1, 2, 3, 4 superposition

$H^{\otimes 2} |0\rangle_2 \; I^{\otimes 2} |0\rangle_2 = \frac{1}{\sqrt{4}} \left[|0\rangle + |1\rangle + |2\rangle + |3\rangle \right] |0\rangle_2$

$\downarrow U_f$ (oracle operation)

$\frac{1}{\sqrt{4}} \left[|0\rangle|a\rangle + |1\rangle|b\rangle + |2\rangle|a\rangle + |3\rangle|b\rangle \right]$

$\downarrow \quad \downarrow$

$x \quad f(x)$

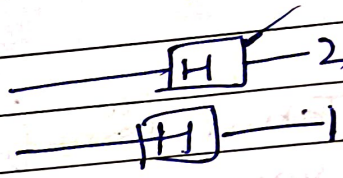
Separated 1st & 2nd reg $\rightarrow = \frac{1}{\sqrt{4}} [|a\rangle] \cdot \frac{1}{\sqrt{2}} \left[\frac{|0\rangle + |3\rangle}{\sqrt{2}} |a\rangle + \frac{|1\rangle + |2\rangle}{\sqrt{2}} |b\rangle \right]$

PEARSONS

If we make measurement on 2nd reg we get
$|a\rangle$ or $|b\rangle$
If $|a\rangle$ first register is collapsed to $\frac{|0\rangle+|3\rangle}{\sqrt{2}}$

again Hadmard on $\frac{|0\rangle+|3\rangle}{\sqrt{2}}$

If 2nd reg is measured we may get
either $|a\rangle$ or $|b\rangle$
Let 2nd register $= |a\rangle$
1st register $\Rightarrow \frac{|0\rangle+|3\rangle}{\sqrt{2}}$



H(0,2)	H(0,1)
H(1,3)	H(2,3)
off on	off on

Hadamard operation on first register

$\downarrow H(0,2)$
$\downarrow H(1,3)$
$(0+2)+(1-3)$

$\downarrow H(0,1)$
$\downarrow H(2,3)$

$\left[\frac{|0\rangle+|3\rangle}{\sqrt{2}}\right]$

2 Hadmard operations

$s.0 = 0$
$s.3 = 0$
$s_1.s_2 = (1\ 1) = 0$
$s_1 + s_2 = 0$
$s_1 = s_2$
11

CLASS	SUBJECT
ROLL NO.	DATE

Let 2nd register $|b\rangle$

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

Apply hadamard on first register

H.

$(1+3)+(0-2)$

H

$\frac{|0\rangle - |3\rangle}{\sqrt{2}}$.

$S \cdot 0 = 0$

$S \cdot 3 = 0$

$S = 11$

Neat

$f(x) = (x \oplus s)$

→ let $s = |11\rangle = |3\rangle_2$

→ $0 \oplus 3 = 3$

$1 \oplus 3 = 2$

$2^1 \quad 2^0$

1 1

$2+1 = 3$

ROLL NO. | SUBJECT | DATE

Simon's Algorithm

f(x) is having some hidden periodicity

f(x): 2 → 1 (It maps 2 inputs for every 1 op)

x	f(x)
x_1	$f(x_1)$
⋮	
x_2	$f(x_2)$

If $f(x_1)=f(x_2) \Rightarrow x_2 = x_1 \oplus s$

↳ Hidden periodicity

Bitwise binary addition

Bit wise binary addition

$(x_1 x_2 x_3) \oplus (y_1 y_2 y_3) = (x_1+y_1)(x_2+y_2)(x_3+y_3)$

↳ mod 2 ↳ mod 2 ↳ mod 2

Examples:- Binary notation

Ex1: $(110) \oplus (101) = (1+1)(1+0)(0+1)$ (mod 2 each)

$= 011$

Ex2: Decimal Notation

① $|6\rangle \oplus |5\rangle = 3 = 011$

$(4+2+0) \oplus (4+0+1) \Rightarrow 3$

Cancel common no

② $|7\rangle_3 \oplus |5\rangle_3 = (4+2+1) \oplus (4+0+1) = 2$

$|7\rangle_3 \oplus |5\rangle_3 = 2 \Rightarrow 2^2 2^1 2^0 \Rightarrow 010$

$|10\rangle_4 \oplus |15\rangle_4 = 2^3 2^2 2^1 2^0 \Rightarrow 5 \Rightarrow 0101$

$(8+0+2+0) \oplus (8+4+2+1)$

EBSONS

3. 2'2
11

$f(x_1) = f(x_2) \Rightarrow x_2 = x_1 \oplus s$ → Hidden Periodicity

① Let $s = |11\rangle = |3\rangle_2$

x	f(x)
0	a
1	b
2	b
3	a

$0 \oplus 3 = 3$ 0 and 3 same o

$1 \oplus 3 = 2$ 1 and 2 same o

$\{a+b\} \in \{0 \text{ to } 3\}$

↳ $a+b$

$a, b \in \{0,1,2,3\}$

$a \neq b$

② $s = |10\rangle = |2\rangle_2$

$0 \oplus 2 = 2$ 0 and 2 same output

$1 \oplus 2 = 3$ 1 and 3 same output

x	f(x)
0	a
1	b
2	a
3	b

③ $s = |110\rangle = |6\rangle_2$

$0 \oplus 6 = 6$

$1 \oplus 6 = 7$

$2 \oplus 6 = 4$

$3 \oplus 6 = 5$

$5 \oplus 6$

x	f(x)
0	a
1	b
2	c
3	d
4	c
5	d
6	a

$\{a,b,c,d\} \leftarrow \{0 \text{ to } 7\}$

↳ Distinct

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

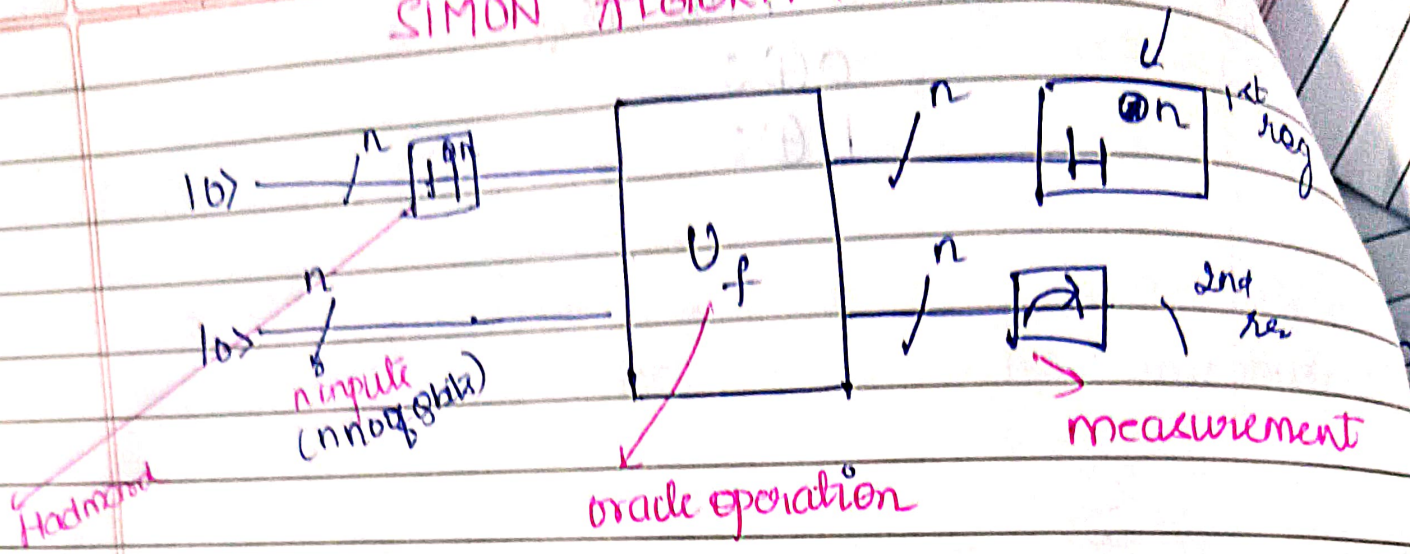
$S = |101\rangle = |5\rangle_3$

$0 \oplus 5$

$1 \oplus 5$

$f(x_1) = f(x_2) \Rightarrow x_2 = x_1 \oplus s$

SIMON ALGORITHM



U_f (oracle function)

$$|x\rangle_n \cdot |0\rangle_n \xrightarrow{U_f} |x\rangle_n |f(x)\rangle$$

$$H^{\otimes n}|0\rangle_n \; I^{\otimes n}|0\rangle_n \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle_n \xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle_n$$

(create superposition)

x	f(x)
z	f(z)
z⊕s	f(z)

same output

Same o/p

(2)

$$\rightarrow \frac{1}{\sqrt{N}} \left[\; + \; + \left(|z\rangle + |z \oplus s\rangle \right) |f(z)\rangle \; + \; + \; \right]$$

$\sqrt{2}$

first register

second register

If 2nd register is measured $\Rightarrow |f(z)\rangle$

First register is collapsed to $\frac{|z\rangle + |z \oplus s\rangle}{\sqrt{2}}$

ROLL NO. | DATE

Hadamard operation on 1st reg $\Rightarrow H^{\otimes n}\left[\frac{|z\rangle + |z \oplus s\rangle}{\sqrt{2}}\right]$

$$= \frac{1}{\sqrt{2}\sqrt{N}}\left[\sum_{y=0}^{N-1}(-1)^{y\cdot z}|y\rangle_n + \sum_{y=0}^{N-1}(-1)^{y\cdot(z\oplus s)}|y\rangle\right]$$

$$= \frac{1}{\sqrt{2N}}\sum_{y=0}^{N-1}\left[(-1)^{y\cdot z} + (-1)^{y\cdot(z\oplus s)}\right]|y\rangle_n$$

$y\cdot z + y\cdot s$

$$\Rightarrow \frac{1}{\sqrt{2N}}\sum_{y=0}^{N-1}(-1)^{y\cdot z}\left[1 + (-1)^{y\cdot s}\right]|y\rangle_n$$

amp to $|y\rangle_n$

$y\cdot s = 0$ → any of $|y_n\rangle = 0$

$y\cdot s = 0$ → amp of $|y_n\rangle \neq 0$

$y\cdot s = 0$ ⇓ System of linearly independent equations to solve (s)

Simon Algorithm Examples

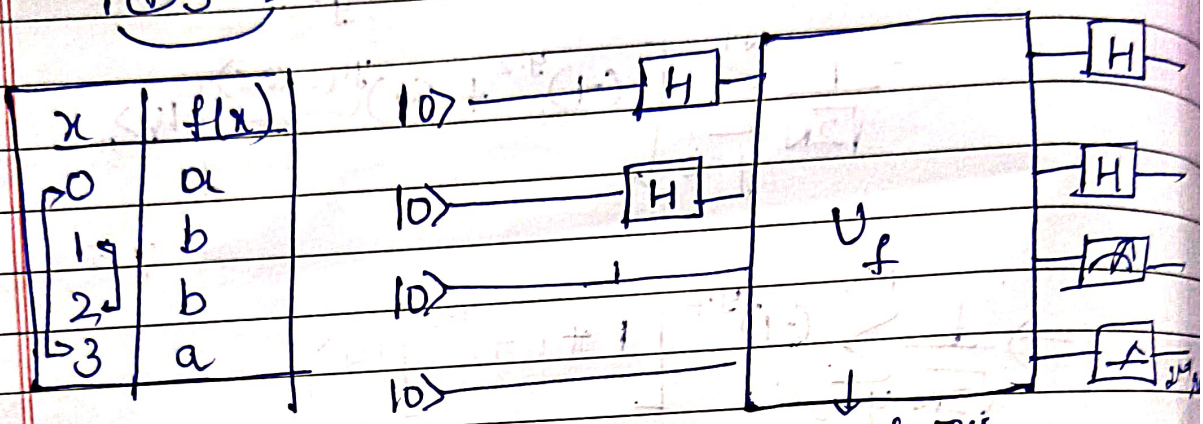
$f(x) = f(x \oplus s)$

a) $s = |1\rangle = |3\rangle_2$

$0 \oplus 3 = 3$

$1 \oplus 3 = 2$

x	f(x)
0	a
1	b
2	b
3	a



$|x\rangle_2 |0\rangle_2 \xrightarrow{U_f} |x\rangle |f(x)\rangle$

$H^{\otimes 2} |0\rangle_2 \; I^{\otimes 2} |0\rangle_2 = \frac{1}{\sqrt{4}} \left[|0\rangle + |1\rangle + |2\rangle + |3\rangle \right] |0\rangle_2$

$\downarrow U_f$

$\Rightarrow \frac{1}{\sqrt{4}} \left[|0\rangle|a\rangle + |1\rangle|b\rangle + |2\rangle|b\rangle + |3\rangle|a\rangle \right]$

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

2^{nd} register 2^{nd} register

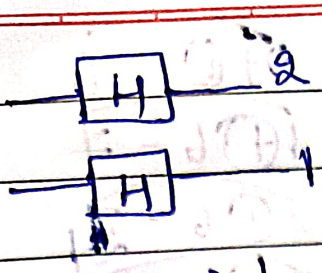
If 2^{nd} register is measured $\Rightarrow$ we may get either $|a\rangle$ or $|b\rangle$

Let 2^{nd} Reg $= |a\rangle$

1^{st} Reg $\Rightarrow \frac{|0\rangle + |3\rangle}{\sqrt{2}}$

CLASS | SUBJECT

ROLL NO. | DATE



H(0,2) | H(0,1)

H(1,3) | H(2,3)

Hadmard operation on 1st reg

H(0,2)

H H(1,3)

(0+2)+(1-3)

H | H(0,1)
H(2,3)

$\frac{|0\rangle + |3\rangle}{\sqrt{2}}$ | $S \cdot 0 = 0$

$S \cdot 3 = 0$

$S \cdot 0 = 0$ | $(S_1 S_2)(11) = 0$

$S_1 + S_2 = 0 \Rightarrow S_1 = -S_2$

Let 2nd register $= |b\rangle$

1st Reg $\Rightarrow \frac{|1\rangle + |2\rangle}{\sqrt{2}}$

H

(1+3)+(0-2)

H

$\frac{|0\rangle - |3\rangle}{\sqrt{2}}$

Σ 2 2 2 2 $\quad 2^3\ 2^2\ 2^1$

0 0 0 1 $\quad$ 0 1 1 0

(0+0+0+1) $\quad$ (0+4+2+0)

Example: $S = |110\rangle = |6\rangle_3$

x	f(x)
0	a
1	b
2	c
3	d
4	c
5	d
6	a
7	b

$0 \oplus 6 = 6$

$1 \oplus 6 = 7$

$2 \oplus 6 = 4$

$3 \oplus 6 = 5$

$$H^{\otimes 3}|0\rangle_3 \; I^{\otimes 3}|0\rangle_3 = \frac{1}{\sqrt{8}}\left[|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\right]$$

$$= \frac{1}{\sqrt{4}}\left[\frac{|0\rangle+|6\rangle}{\sqrt{2}}|a\rangle + \frac{|1\rangle+|7\rangle}{\sqrt{2}}|b\rangle + \frac{|2\rangle+|4\rangle}{\sqrt{2}}|c\rangle + \frac{|3\rangle+|5\rangle}{\sqrt{2}}|d\rangle\right]$$

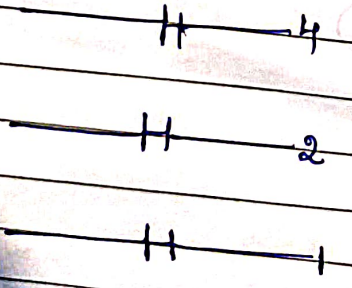
split

If 2nd register is measured we may get

$|a\rangle\ |b\rangle\ |c\rangle\ |d\rangle$

Let 2nd register $= |c\rangle_3$

Let 1st register $= \frac{|2\rangle+|4\rangle}{\sqrt{2}}$



H(0,4)	H(0,2)	H(0,1)
H(1,5)	H(1,3)	H(2,3)
H(2,6)	H(4,6)	H(4,5
H(3,7)	H(5,7)	H(6,7)

left →

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

1st reg = $\frac{|2\rangle_3 + |4\rangle_3}{\sqrt{2}}$

↓ Hadmard

$(|2\rangle + |6\rangle) + (|0\rangle - |4\rangle)$

↓ Hadmard

$|0\rangle - |6\rangle$

↓ Hadmard

$[(|0\rangle + |1\rangle) - (|6\rangle + |7\rangle)]$

$= \frac{1}{\sqrt{4}} [|0\rangle + |1\rangle - |6\rangle - |7\rangle]$

Bit flip error

→ Definition: Bit flip error occurs when qbit changes from $|0\rangle$ to $|1\rangle$ or viceversa

Pauli X operator - Bit flip error operator

→ Steps:- Transformation - Encoding

Syndrome - Detection measurement done by parity check

Correction - Use quantum gates which do not disturb original gates.

→ For state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ Bit flip swaps the amplitudes of $|0\rangle$ and $|1\rangle$ state.

1] **Transformation** - Encoding → 9 bit Encoding

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

Logical $|0\rangle \rightarrow |000\rangle$

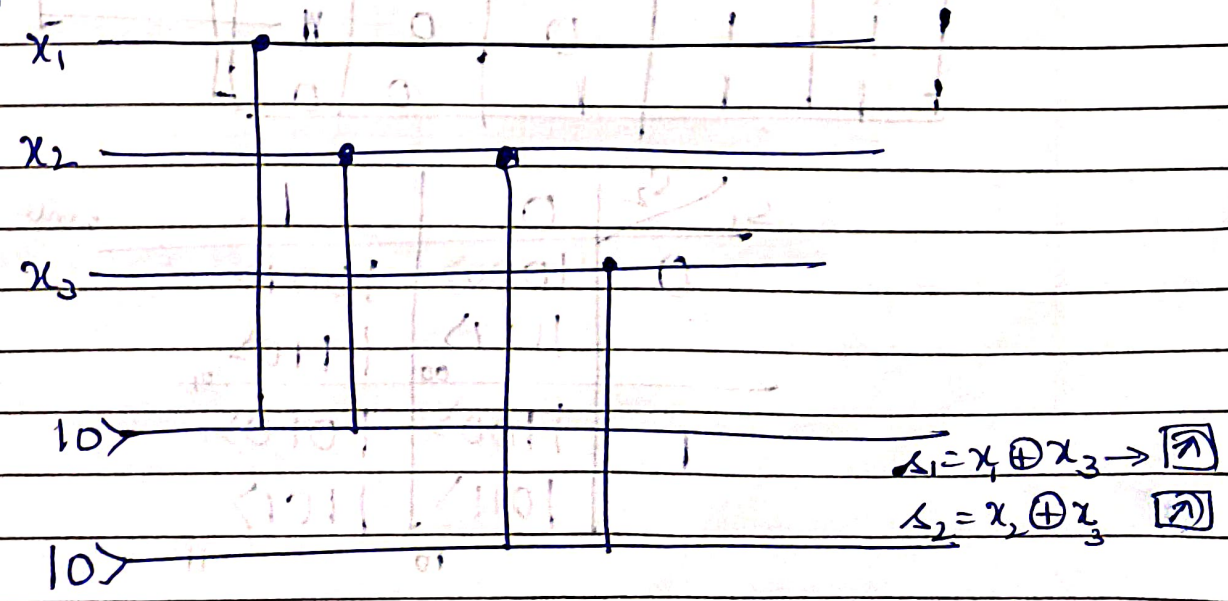
Logical $|1\rangle \rightarrow |111\rangle$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha|000\rangle + \beta|111\rangle$

One logical qbit is encoded into three physical qubits using redundancy.

2] **Syndrome measurement**:-

Two syndrome bits uniquely identify which qbit has the error without collapsing the quantum state.



Ancilla bit - Direct measurement of data qubits would collapse the quantum superposition.

Ancilla bits - Direct measurement of data qubits would collapse the quantum superposition. destroying the quantum information. Ancila Qubits allows us to extract error information (syndrome) while preserving the quantum state of the data qubits.

Data Qubits : $\alpha|000\rangle + \beta|111\rangle$

Ancilla Qubits : $|s_1, s_2\rangle$ (measured gives classical qubits)

s_1	s_2	error
0	0	no error
0	1	3rd bit
1	0	1st bit
1	1	2nd bit

x_1	x_2	x_3	s_1	s_2	
0	0	0	0	0	no error
0	0	1	0	1	3rd bit error
0	1	0	1	1	
0	1	1	1	0	2nd bit
1	0	0	1	0	1st bit
1	0	1	1	1	
1	1	0	0	1	
1	1	1	0	0	

s_1 \ s_2	0	1
0	$\|000\rangle$	$\|001\rangle$
	$\|111\rangle$	$\|110\rangle$
1	$\|100\rangle$	$\|010\rangle$
	$\|011\rangle$	$\|101\rangle$

write

00 01 10 11

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

Stabalizers

Hermiton operator $= A^2 = I$

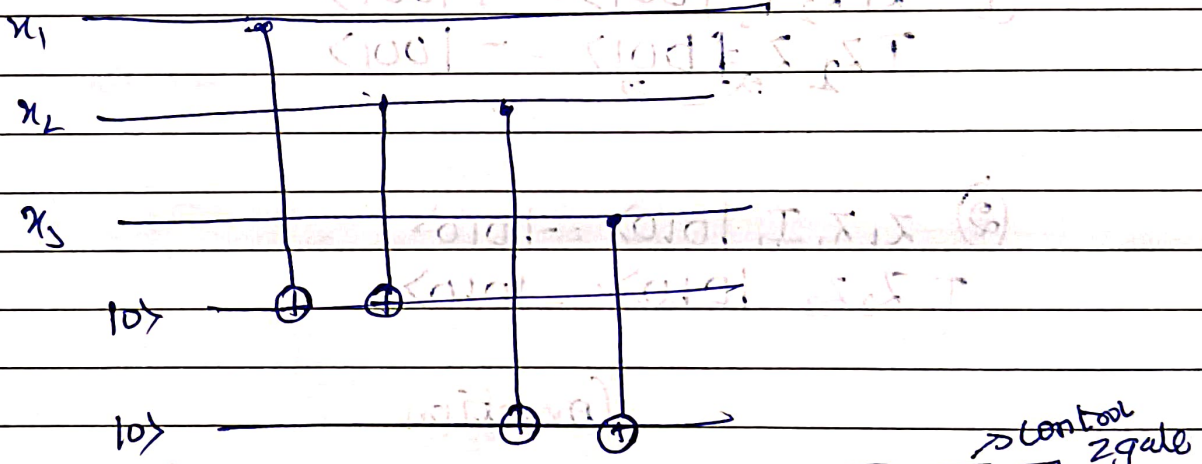
Eigen values $\lambda = \pm 1$

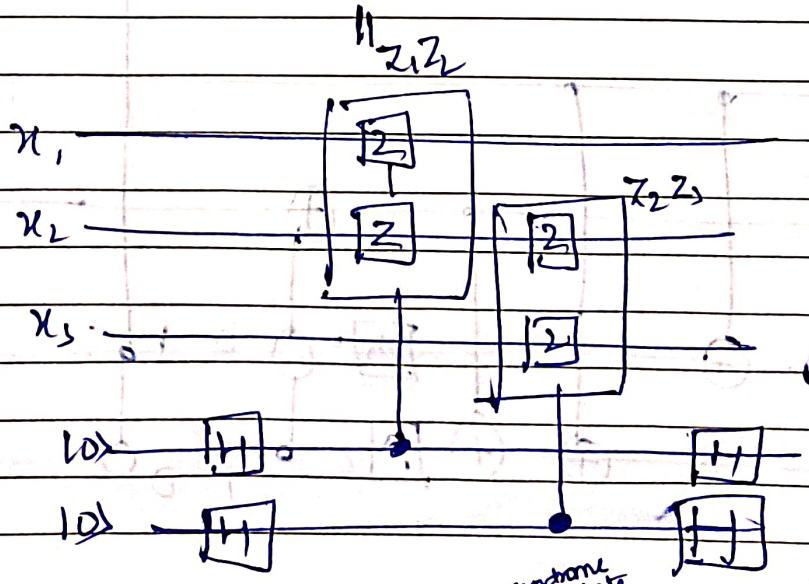
$\hat{S}|\psi\rangle = \pm|\psi\rangle$ → Eigen value are equal to ± 1

↙ Stabalize

↓ Syndrome state

[Eigen value equation]





Stabalizers $Z_1Z_2|\psi\rangle = (-1)^{S_1}|\psi\rangle$ → syndrome state → S_1

$Z_2Z_3|\psi\rangle = (-1)^{S_2}|\psi\rangle$

s_1 \ z_2z_3	0	1
+	000	001
0	111	110
−	100	010
	111	101

z_1z_2

$$z_1z_2|\psi\rangle = (-1)^{s_1}|\psi\rangle$$
$$z_2z_3|\psi\rangle = (-1)^{s_2}|\psi\rangle$$

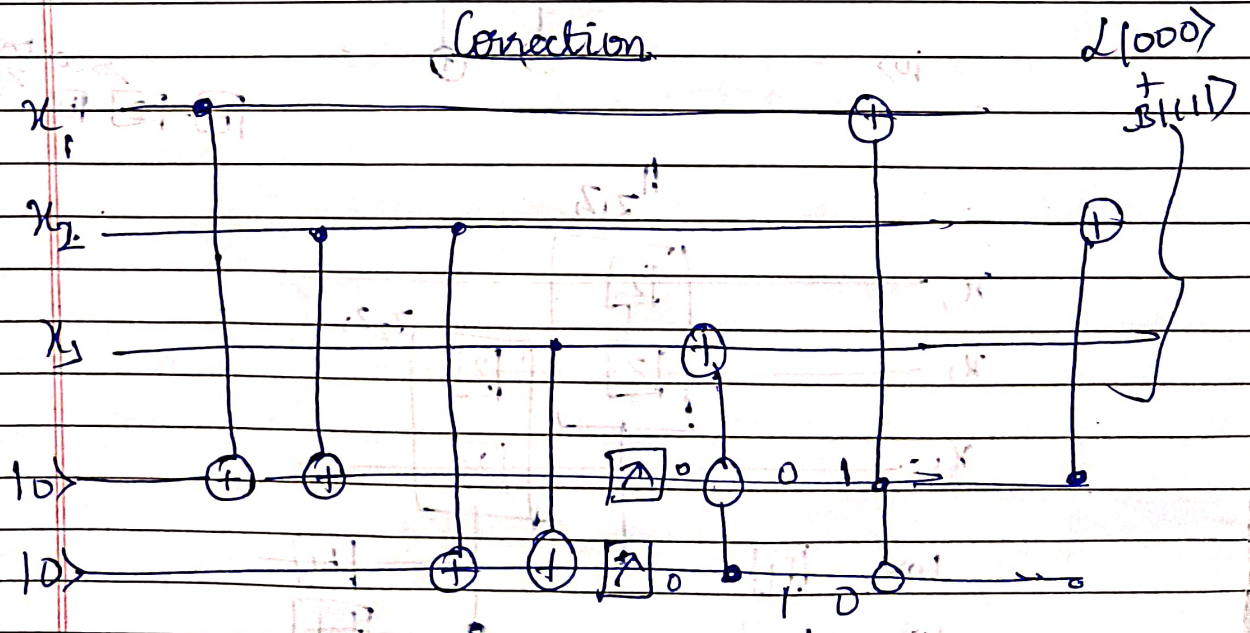
① $z_1z_2I_3|001\rangle = +|001\rangle$

$I z_2 z_3 |001\rangle = -|001\rangle$

② $z_1z_2I_3|010\rangle = -|010\rangle$

$I z_2z_3 |010\rangle = -|010\rangle$

Correction



STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

Phase flip error

↳ No classical analogy

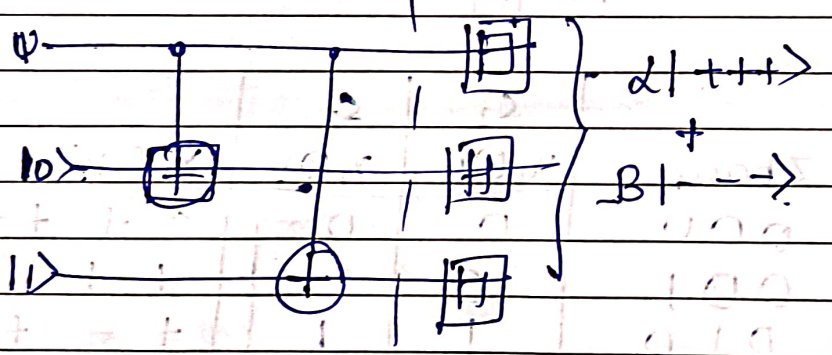
→ Convert phase flip model to bit flip model by transforming the basis.

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

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

$$H|1\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] = |-\rangle$$

Encoded circuit:-



Noise -

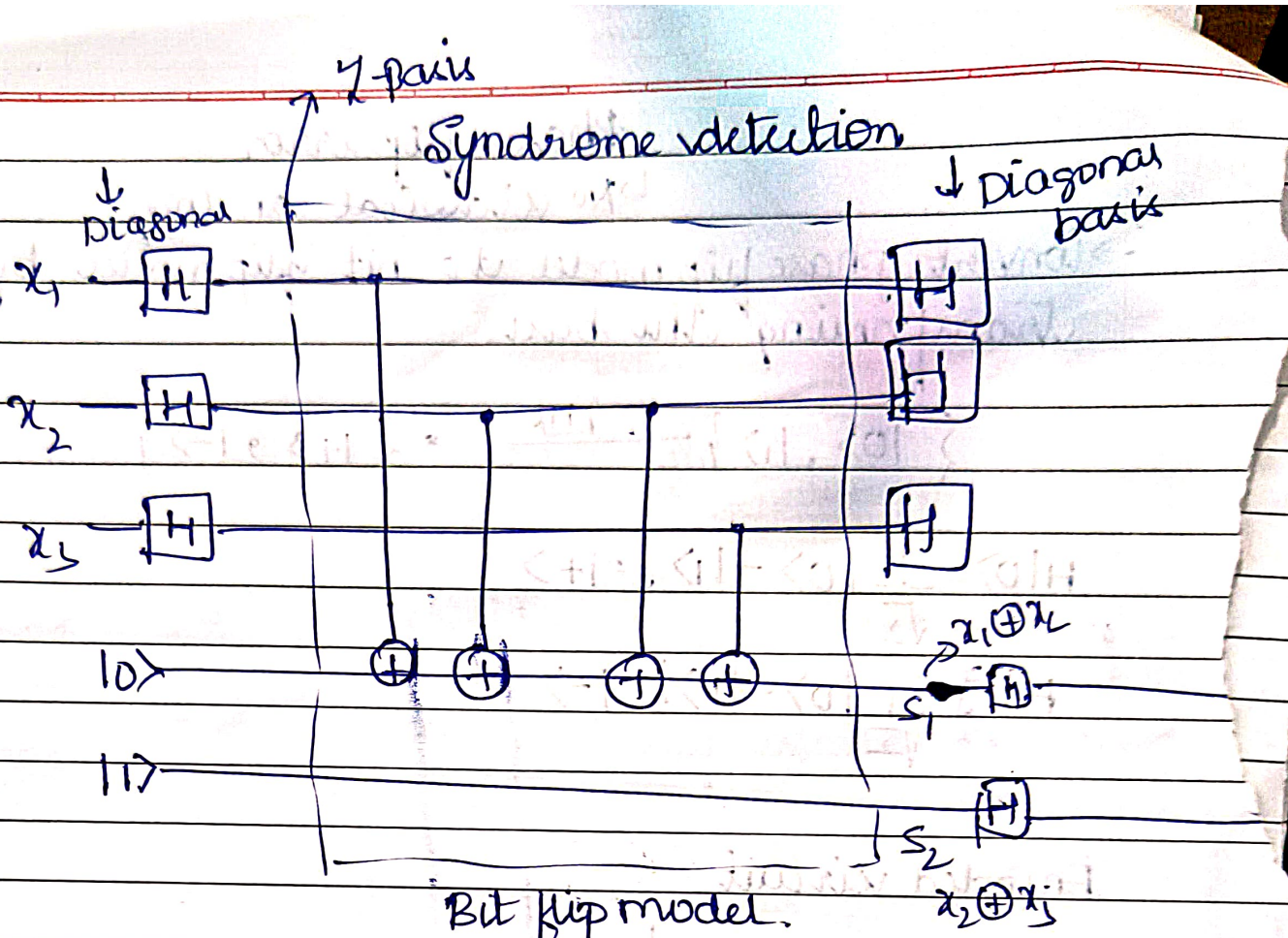
$I \otimes I \otimes I$ → no error

$Z \otimes I \otimes I$ → 1st Qubit

$I \otimes Z \otimes I$ → 2nd Qubit

$I \otimes I \otimes Z$ → 3rd Qubit

EBSONS



Bit flip model.

$x_1\ x_2\ x_3$ X Basis	Z basis	s_1 $x_1 \oplus x_2$	s_2 $x_2 \oplus x_3$	X Basis
+ + +	000	0	0	+ + +
+ + −	001	0	1	+ + −
+ − +	010	1	1	+ − +
+ − −	011	1	0	+ − −
− + +	100	1	0	− + +
− + −	101	1	1	− + −
− − +	110	0	1	− − +
− − −	111	0	0	− − −

No error

No error

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

S_1 \ S_2	0	1
0	+++	++−
	−−−	−−+
1	−++	+−+
	+−−	−+−

Stabalizers :-

$X_1X_2|\psi\rangle = \pm|\psi\rangle$

$X_2X_3|\psi\rangle = \pm|\psi\rangle$

x_1x_2 \ S_1 \ S_2	+	−
+ 0	+++	++−
	−−−	−−+
− 1	−++	+−+
	+−−	−+−

$X_1X_2|\psi\rangle = (-1)^{S_1}|\psi\rangle$

$X_2X_3|\psi\rangle = (-1)^{S_2}|\psi\rangle$

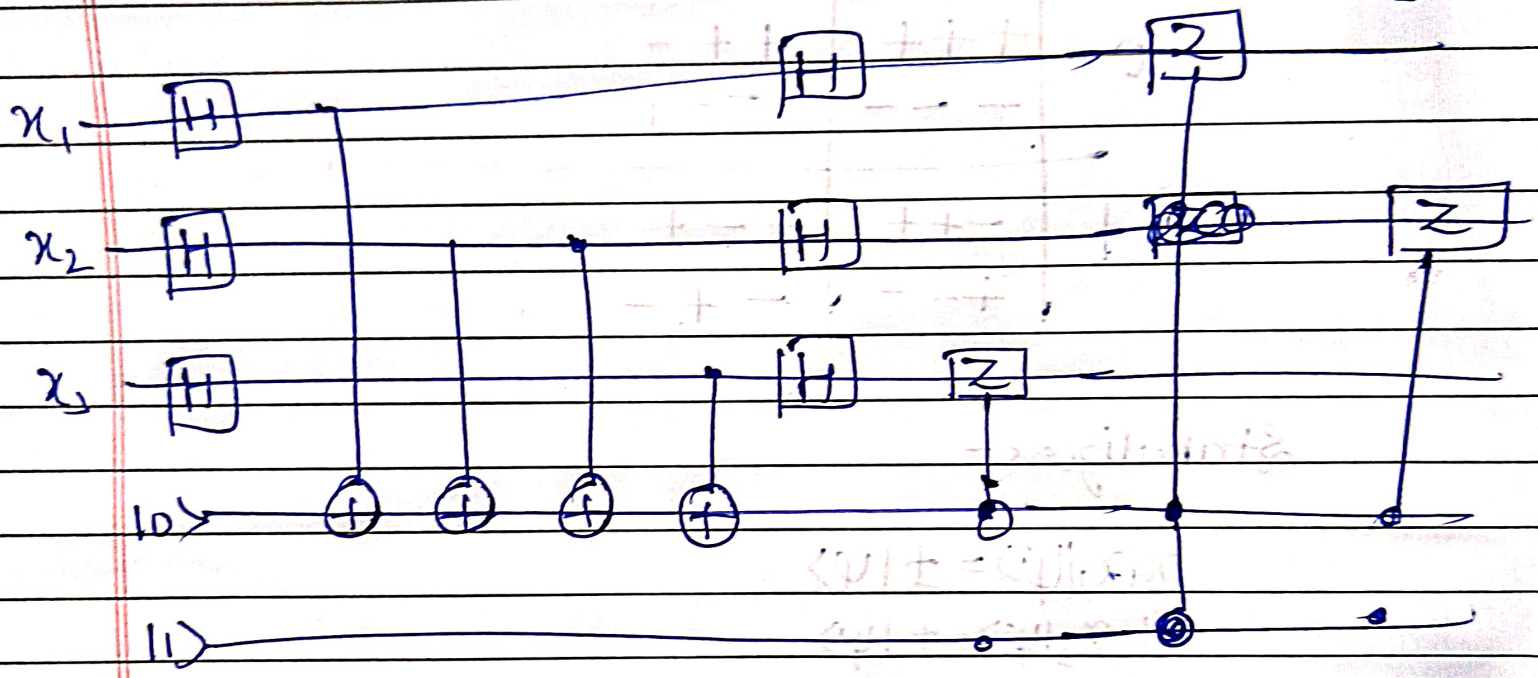
$X_1X_2|+++\rangle = +|+++\rangle$

$X_2X_3|---\rangle = +|---\rangle$

$X_1X_2|+-+\rangle = -|+-+\rangle$

$X_2X_3|+-+\rangle \quad -|+-+\rangle$

Correction



STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

QKD

QKD is based on 2 key concepts

- Superposition
- Measurement disturbance

↓ Measuring the quantum state disturbs it revealing the presence of an eavesdropper [Eve]

↓ eves dropper measure

Alice ——————— Bob

two basis

rectilinear / diagonal

→ Preparation
→ Transmission
→ Measurement
→ Basis Reconciliation
→ Key sifting & error check.

Explain with App

share link

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

Shor code

→ Shor code is a quantum error that corrects one logical bit into 9 physical bits to protect it from bit flip and phase flip error.

→ The code works by using a repetative pattern of encoding and entanglement across the nine qubits to detect and correct errors without directly measuring logical bit.

Working of shor code
Step 1:- Transformation - encoding
Step 2:- Syndrome measurement
Step 3:- Error correction

Transformation:-

→ First apply modified version of the 3 bit repetation code which detect phase flip error and then we will encode each of the resulting three bits independently using the original 3 bit repetation code which detects phase flip errors

Step 1 → A single Qubit in unknown state

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

Create three copies.

$$|0_L\rangle = |000\rangle \; , \; |1_L\rangle = |111\rangle$$

After encoding

$$|\psi\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

Step 2 Encode each of the Three Qubits again

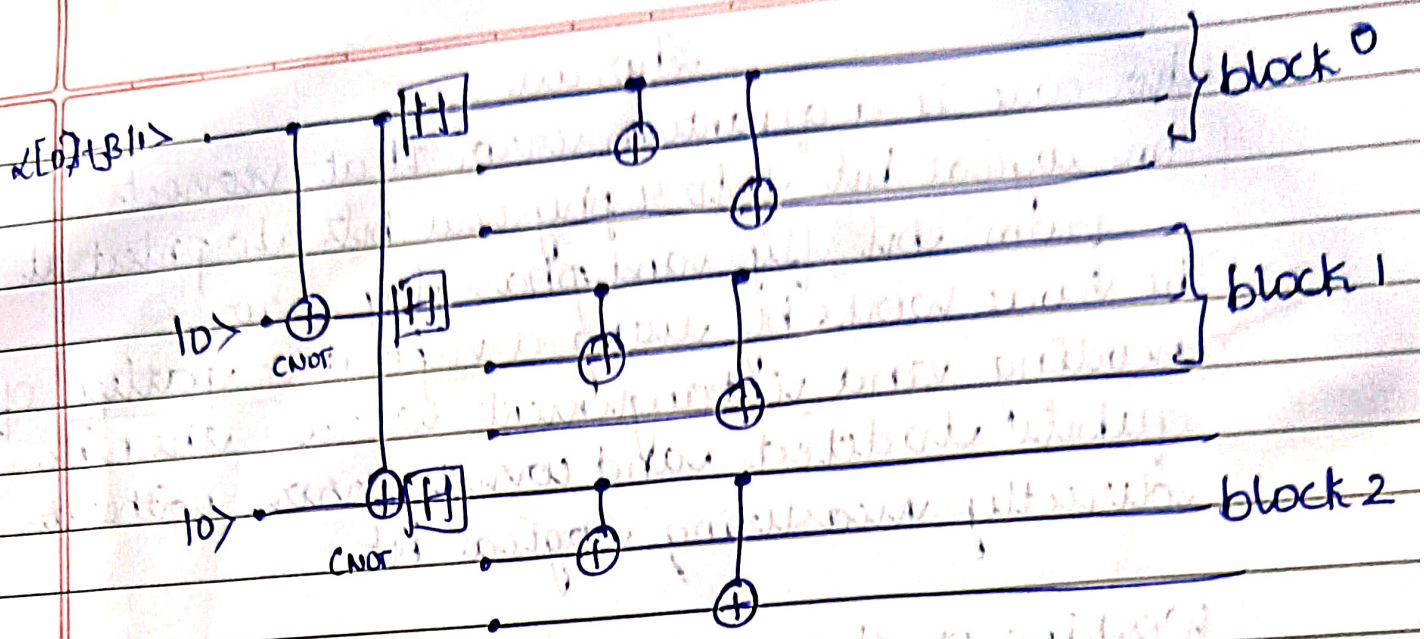
$$|000\rangle \rightarrow \frac{1}{2}|000\rangle + |111\rangle^{\otimes 3}$$

$$|111\rangle \rightarrow \frac{1}{2}|000\rangle + |111\rangle^{\otimes 3}$$

The nine Qubit encoded state

$$|\psi\rangle \rightarrow \frac{\alpha}{2}(|000\rangle + |111\rangle)^{\otimes 3} + \frac{\beta}{2}|000\rangle - |111\rangle^{\otimes 3}$$

EBSONS



→ Inner code – 3 bit repetation code
→ Outer code → First encoding

Syndrom detections - Parity check
Bit flip (z-type) Stabalizers
Phase flip (x-type) stabalizers

Bit flip

$S_1 - Z_1Z_2$
$S_2 - Z_2Z_3$
$S_3 - Z_4Z_5$
$S_4 - Z_5Z_6$
$S_5 - Z_7Z_8$
$S_6 - Z_8Z_9$

Phase flip:

$S_7 = X_1X_2X_3X_4X_5X_6$
$S_8 = X_4X_5X_6X_7X_8X_9$

STUDENT'S NAME		TO OBTA
CLASS	SUBJECT	
ROLL NO.	DATE	

UNIT 3

For ∞ Steane Quantum error correction

→ Quantum information is extremely fragile due to coherence and noise.

→ Quantum error correction provides methods to detect and correct errors without measuring or disturbing quantum information

→ One of the important QEC code is the steane code also called [7, 1, 3] CSS code.

→ It was proposed by Andrew steane 1996

→ It protects 1 logical qubit using 7 physical qubits and can correct any single qubit errors.

→ Error types → Bit flip error $|0\rangle \leftrightarrow |1\rangle$
Phase flip error $|+\rangle \leftrightarrow |-\rangle$
Combined error $Y = iXZ$.

Steane code detects and corrects all three errors

(1)

→ Steane code is a CSS (Calder-Shor-Steane) code constructed using two classical linear codes

Hamming [7, 4] dual code

↳ Hamming encode classical 4 bits into 7 bits
↳ Detects and corrects 1 classical bit/flip error
↳ Defined by parity check matrix

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

Steane uses this code to built the quantum stabalizers

→ Encoding

Structure of Steane code

[7, 1, 3]

7 → 7 Physical bits

1 → 1 logical bit

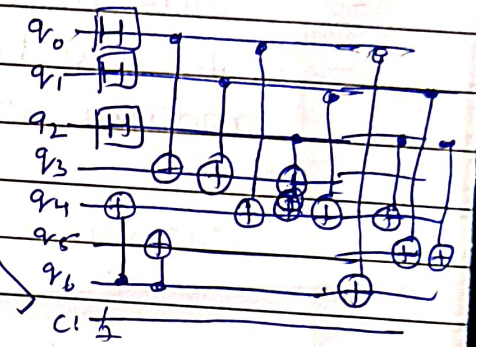
3 → Distance 3 → can correct one errors.

Logical States

Logical states are superposition of all valid Hamming codewords

$$|0_L\rangle = \frac{1}{\sqrt{8}} \sum_{c \in C} |c\rangle$$

$$|1_L\rangle = \frac{1}{\sqrt{8}} \sum_{c \in C} |c \oplus 1111111\rangle$$



Ensures both bit flip & Phase flip protection

→ CNOT / Hadamard / Hamming code → Circuit

→ Syndrome.

To detect errors ancillary qubits are used to measure stabalizers

X type stabalizers - Detect Z phase errors

Z type stabalizers - Detect X bit errors

6 stabalizers

X type stabalizers

$S_1 - X_1 X_2 X_3 X_1 -$

$S_2 - X_1 X_3 X_4 X_6$

$S_3 - X_2 X_3 X_4 X_7$

Z type stabalizers

$S_4 - Z_1 Z_2 Z_3 Z_5 -$

$S_5 - Z_1 Z_3 Z_4 Z_6$

$S_6 - Z_3 Z_3 Z_4 Z_7$

Derived from Hamming code

STUDENT'S NAME		TOTAL MARKS OBTAINED
CLASS	SUBJECT	
ROLL NO.	DATE	

Syndrome table

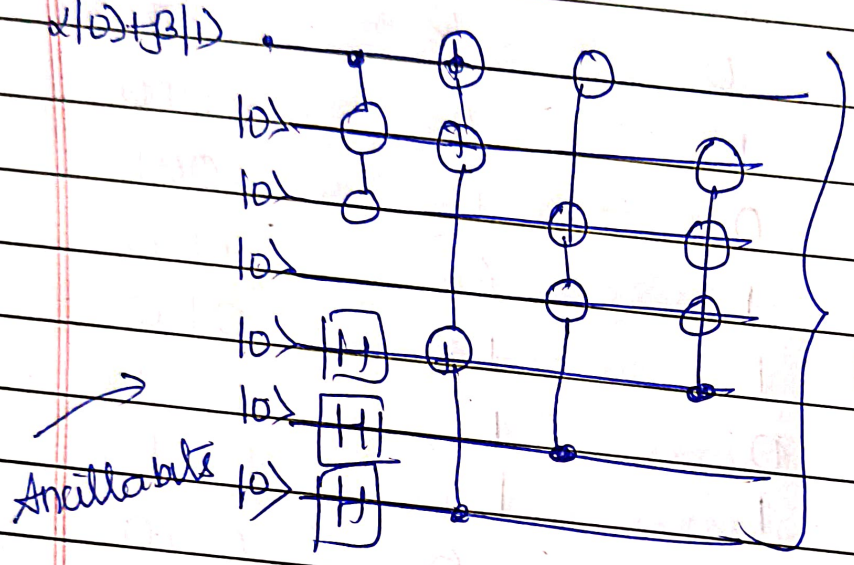
Qubit	M1	M2	M3	Syndrome
1	1	0	0	100
2	0	1	0	010
3	0	0	1	001
4	1	1	0	110
5	0	1	1	010
6	1	0	1	101
7	1	1	1	111
No error	0	0	0	000

If we measure 100 → flip Qbit 1
If we measure 010 → flip Qubit 5
↑ same table for phase error.

Error correction:-

→ Apply the inverse operation to restore the correct encoded state
→ If a bit flip is detected apply X on faulty bit
→ If a phase flip is detected apply Z on faulty bit
→ If combined error is detected apply Y
→ After correction the logical qubit returns to $|\psi_L\rangle$

Encoder for Steane's code



NARAYANA EDUCATIONAL INSTITUTIONS
.....Creating Global Leaders
CBSE
Branch : .....
EXAMINATION : .....
Date : .....
Name : Kum / Master .....
Max. Marks : .....
I.D. No. : ..... Subject : ..... Class / Sec : .....
Time : .....
Signature of Invigilator .....
(With date)
Sign. of Evaluator .....
(With date)

Hamming code.

Steam code :- [7, 1, 3] CSS quantum error correcting code.
- 7 → physical bit
- 1 → logical bit
- 3 → distance [corrects one qubit error]

Build from Hamming code.

X, Z & Y errors

Hamming code :- encode 4 bits to 7 bits

Parity check matrix :- $H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$ ← Parity checks

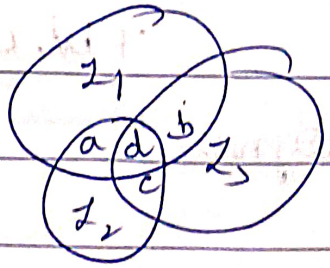
bit position

Steam uses this matrix for X & Z stabalizers

4 bit message → a, b, c, d → original
Parity check bits → z_1, z_2, z_3

[7, 4]
- 7 → encoded bits
- 4 → logical bits

$z_1 = a \oplus b \oplus d$
$z_2 = a \oplus c \oplus d$
$z_3 = b \oplus c \oplus d$
} mod 2 → XOR



Bit position	1	2	3	4	5	6	7
Parity bit arrangement	P1	P2	D1	P3	D2	D3	D4
	LSB1	LSB2		LSB3			

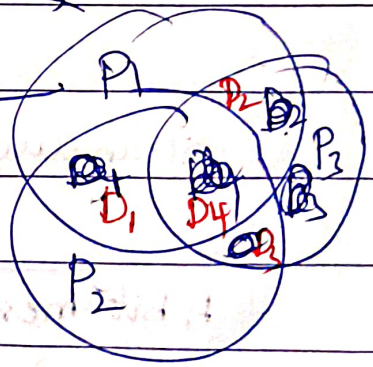
Position	Binary
1	001
2	010
3	011
4	100
5	101
6	110
7	111

4 2 1

P1 → 1 3 5 7 → $P_1 = b_1 \oplus b_3 \oplus b_5 \oplus b_7$

P2 → 2 3 6 7 → $P_2 = b_2 \oplus b_3 \oplus b_6 \oplus b_7$

P3 → 4 5 6 7 → $P_3 = b_4 \oplus b_5 \oplus b_6 \oplus b_7$



$P_1 = D_1 \oplus D_2 \oplus D_4$

$P_2 = D_1 \oplus D_3 \oplus D_4$

$P_3 = D_2 \oplus D_3 \oplus D_4$

1 2 3 4 5 6 7

7 bit code → $P_1\ P_2\ D_1\ P_3\ D_2\ D_3\ D_4$

Syndrome: 3 bit no

000 No error

101 → bit 5 error

011 → bit 3 error

110 – bit 6 error

Ex: $D_1=1, D_2=0, D_3=1, D_4=1$

$1 \oplus 0 = 0 \bmod 2$
$= 0+1$

$P_1 = 1 \oplus 0 \oplus 1 = 0$

$P_2 = 1 \oplus 1 \oplus 1 = 1$

$P_3 = 0 \oplus 1 \oplus 1 = 0$

$P_1 P_2 D_1 P_3 D_2 D_3 D_4$

Codeword - 0110011

syndrom = 101 = 5 bit flip

0110011
0100011

Steam - 7 1 3

P ↙ Loss ↘ 3

bit positions

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

Parity

Introduction to Quantum Teleportation

Objectives

- Explain what teleportation *is* and *is not*.
- Remove misconception: physical matter is not teleported.

Points to cover

- Quantum teleportation: *transfer of an unknown quantum state* from one location to another **without physically sending the particle**.
- Requires two resources:
    1. **Quantum entanglement**
    2. **Classical communication**
- Used in:
    - Quantum internet
    - Distributed quantum computing
    - Long-distance qubit transfer

Prerequisits

1. Qubits (5 min)

- Represented as

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

2. Dirac Notation Refresher (5 min)

- Ket, Bra, Tensor product
- Measurement: state collapse

3. Entanglement (10 min)

- Definition: State of combined system cannot be factored.

The Bell States (Core of teleportation)

Define the 4 Bell States

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

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

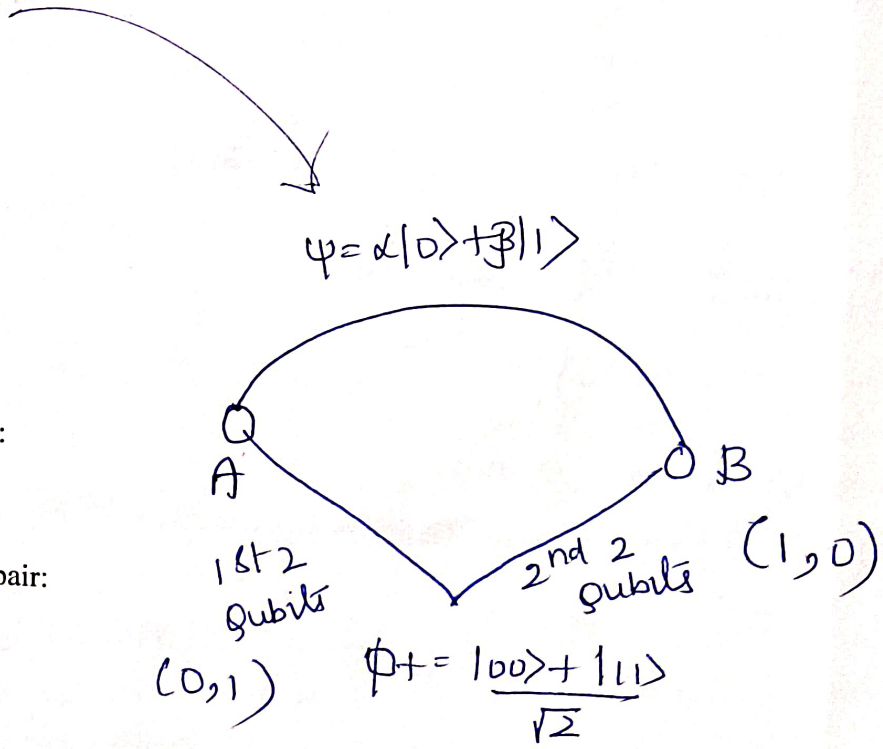
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

key properties

- Maximal entanglement
- Measurement of one determines the other
- Cannot be prepared by local operations

Simple Diagram



Characters

- **Alice** (sender)
- **Bob** (receiver)

Initial Resources

- Alice has unknown state:

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

- Alice & Bob share Bell pair:

System label

Q1.

- Qubit 1: Unknown state (Alice)
- Qubit 2: Alice's half of Bell pair
- Qubit 3: Bob's half of Bell pair

STEP 1 — Combine unknown qubit with Bell pair

Full state:

$|\psi\rangle \otimes |\Phi+\rangle$

Expand: $\psi = \beta_{00} = [\alpha|0\rangle + \beta|1\rangle] \otimes \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$

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

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

Explain tensor-product expansion clearly.
This is the **raw starting point.**

STEP 2 — Alice applies CNOT on (1→2)

x	y	CNOT
0	0	00
0	1	01
1	0	11
1	1	10

- Control: qubit 1
- Target: qubit 2

Show effect:

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

Resulting 3-qubit state:

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

STEP 3 — Alice applies Hadamard on qubit 1

Hadamard

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

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

Hadamard acts as:

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

$= \frac{1}{\sqrt{2}}[\alpha|+00\rangle + \alpha|+11\rangle + \beta|-10\rangle + \beta|-01\rangle$

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

Interpretation

- Measurement results (00, 01, 10, 11) determine which version of **Bob's qubit** he will receive.

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

$|00\rangle_A = \alpha|0\rangle+\beta|1\rangle \qquad |01\rangle = \alpha|1\rangle+\beta|0\rangle$

$|10\rangle_A = \alpha|0\rangle-\beta|1\rangle \qquad |11\rangle = \alpha|1\rangle-\beta|1\rangle$

Diagram:

Alice: [Q1: ψ] — CNOT — H — Measure ——— classical bits ——▶ Bob
Bob: apply correction

STEP 4 — Alice measures qubits 1 and 2 (Bell basis)

Possible outputs:

- 00
- 01
- 10
- 11

Each occurs with probability 1/4.

Bob's qubit collapses accordingly:

Corresponding collapsed states

Alice outcome	Bob receives	
00	(\alpha	$\alpha\|0\rangle+\beta\|1\rangle$
01	(\alpha	$\alpha\|1\rangle+\beta\|0\rangle$
10	(\alpha	$\alpha\|0\rangle-\beta\|1\rangle$
11	(\alpha	$\alpha\|1\rangle-\beta\|1\rangle$

STEP 5 — Alice sends 2 classical bits to Bob

Explain:

- Shows quantum teleportation is **not faster than light.**
- Classical communication ensures causality.

STEP 6 — Bob applies correction operations

Outcome	Correction	Meaning	
00	I	Do nothing	$\longrightarrow \alpha\|0\rangle+\beta\|1\rangle$

Outcome	Correction	Meaning
01	X	Bit flip
10	Z	Phase flip
11	ZX	Bit + Phase flip

$\alpha|1\rangle+\beta|1\rangle \xrightarrow{X} \alpha|0\rangle+\beta|1\rangle$

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

$\alpha|1\rangle-\beta|0\rangle \xrightarrow{XZ} \alpha|0\rangle+\beta|1\rangle$ } ψ

Explain Pauli gates:

- **X gate:** $|0\rangle \leftrightarrow |1\rangle$
- **Z gate:** $|1\rangle \rightarrow -|1\rangle$

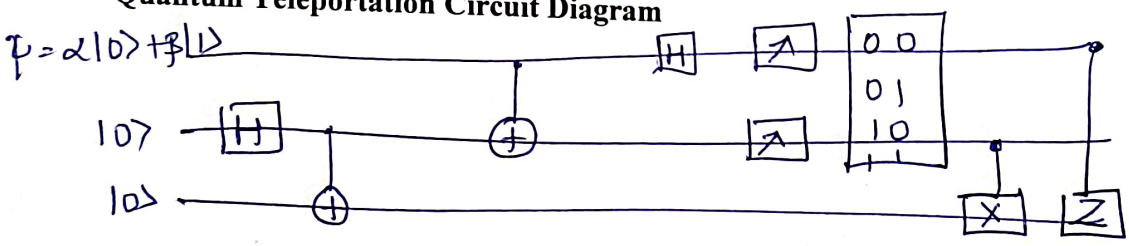
STEP 7 — Bob reconstructs the unknown state

After applying the correction:

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

Teleportation complete.

Quantum Teleportation Circuit Diagram



- b1, b2 are measurement results.

Applications

- Quantum repeaters
- Quantum internet nodes
- Distributed quantum computing
- Secure communication (with QKD + teleportation)

Extensions to teach

- Teleportation of multi-qubit states
- Continuous-variable teleportation
- Entanglement swapping
- GHZ state teleportation

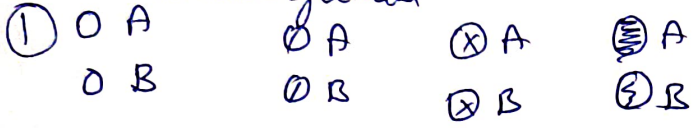
Entanglement

Bell Measurement

Classical Communication.

State reconstruction

Entanglement



(2) A secret state card
(Unknown 9 bit)

(3) Two small cards

0

1

Quantum computing deals with density matrix, pure/mixed states and superpositions quantum analog.

Von entropy is that measure which help us analyze
- Pure Quantum states
- Entanglement
- Noise & decoherence
- Quantum channel capacity
- Quantum thermodynamics

1. Entropy (S(A)) — Measure of Uncertainty

- **Formal definition**

$$S(A) = -tr(\rho_A \log \rho_A)$$

$$S(\rho) = -\sum_i \lambda_i \log \lambda_i$$

$\lambda_i \rightarrow$ eigen values of density matrix

- **Simple meaning**

Entropy measures **how uncertain, unpredictable, or mixed** a system is.

- **HR example**
  - A team where everyone has **clear job roles** → low entropy (less uncertainty).
  - A team where responsibilities are mixed and unclear → high entropy.

- **Quantum meaning**

Entropy tells how **mixed** a quantum state is.

Low entropy → state is pure → full knowledge.
High entropy → state is mixed → uncertainty.

$S(\rho) = 0$ Pure state ↓ entropy

$S(\rho) = 1$ Mixed state ↑ entropy

Why Do We Need Von Neumann Entropy in Quantum Computing?

✓ To measure how much **quantum information** is present
✓ To quantify **entanglement**
✓ To know how much **noise** or **disturbance** a quantum state has
✓ To optimise **quantum algorithms**
✓ To understand **quantum thermal systems**

Concept	Simple Meaning
Quantum state	Many possibilities at once
Density matrix ρ	Distribution of these possibilities
Von Neumann entropy	How uncertain / mixed the quantum state is
Low entropy	Clear, predictable system
High entropy	Confusing, mixed system

Applications:

→ Measuring entanglement
→ Quantifying decoherence
→ Quantum channel capacities
→ Quantum thermodynamics

Entropy, Relative Entropy, Conditional Entropy, Mutual Information, Subadditivity, Strong Subadditivity, and Monotonicity.

Classical Shannon Entropy

Used for *normal probability data*

Example: probability of selecting an employee from a team.

Quantum Von Neumann Entropy

Used when the system is not classical, but a quantum state—
a state that can be a mixture of many possibilities at once.

Formal definition (from your image):

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho)$$

Trace of square matrix is sum of its diagonal elements

Ex: $A = \begin{bmatrix} 2 & 0 \\ 1 & 3 \end{bmatrix}$

$Tr(A) = 2+3 = 5$

Ex: $P = \begin{pmatrix} 0.7 & 0 \\ 0 & 0.3 \end{pmatrix}$

Eigenvalues 0.7, 0.3

$S = -0.7(\log(0.7)$

$-0.3\log(0.3)$

Where ρ (rho) is a density matrix representing a quantum state.

You can think of ρ as "how confused or certain" the system is.

2. Relative Entropy (Kullback–Leibler divergence)

- **Formula**

$$S(\rho \| \sigma) = tr(\rho \log \rho - \rho \log \sigma)$$

- **Simple meaning**

Relative entropy measures **how different one distribution is from another.**

- **HR example**

Comparing:

- expected employee performance (σ)
  vs
- actual performance distribution (ρ)

Large difference → high relative entropy (teams not meeting expected patterns).
Small difference → actual is close to expected.

- **Purpose**

Used to measure "distance" between two states, though not a true distance.

3. Conditional Entropy (S(A|B))

- **Formula**

$S(A|B)=S(A,B)-S(B)S(A|B) = S(A,B) - S(B)S(A|B)=S(A,B)-S(B)$

- **Simple meaning**

"How uncertain A is **if you already know B.**"

- **HR example**
  - If you know an employee's department (B), you can predict tasks (A) better.
  - So uncertainty reduces.

Conditional entropy helps measure **predictability with context.**

- **Quantum twist**

Sometimes S(A|B) can be negative → uniquely quantum!

4. Mutual Information (S(A:B))

- **Formula**

$S(A:B)=S(A)+S(B)-S(A,B)S(A:B) = S(A) + S(B) - S(A,B)S(A:B)=S(A)+S(B)-S(A,B)$

- **Simple meaning**

Mutual information measures **how much A tells you about B.**

- **HR example**
  - Employee attendance and employee productivity might be correlated.
    High mutual information → strong relationship.
    Low mutual information → weak relationship.

- **Quantum meaning**

Quantifies total correlations (classical + quantum).

5. Subadditivity

- **Inequality**

$S(A,B)\leq S(A)+S(B)$ ~~$S(A,B) \leq S(A) + S(B) S(A,B) \leq S(A)+S(B)$~~

- **Meaning**

The uncertainty of a joint system is **never more** than the sum of uncertainties of the individual parts.

- **HR example**

Team performance (A+B) is usually **more organized** than individual random behaviors.
So combined uncertainty is less.

6. Strong Subadditivity

- **Inequality**

$$S(A,B,C)+S(B)\leq S(A,B)+S(B,C)$$

- **Meaning**

This is the most important inequality in quantum information.
It says: **Knowing the middle piece (B) reduces uncertainty the most.**

- **HR example**

Consider A = employee skills
B = training program
C = job performance

Knowing B (training received) reduces uncertainty between skills and performance.
Training acts as the bridge.

7. Relative Entropy is Convex

- **Meaning**

Relative entropy behaves nicely mathematically:

- mixing distributions never reduces divergence
- helpful in optimization and HR analytics

- **HR example**

If you mix two groups of employees, the "difference from expectation" cannot reduce magically.

The combined group still reflects the difference.

8. Monotonicity of Relative Entropy

- **Formula**

$$S(\rho_A \| \sigma_A) \leq S(\rho_{AB} \| \sigma_{AB})$$

- **Meaning**

Processing or ignoring information **never increases information.**

- **HR example**

If you only look at employee performance **without** background data (AB → A),
you cannot get *more* insight than when you had all the data together.

Information decreases when you discard data.

Activity

Real-Life Activity: "The Mystery Box Challenge"

A hands-on way to understand entropy (uncertainty)

Activity Setup (5 minutes)

You need:

- 3–4 **closed boxes** (shoe boxes / opaque containers)
- Inside each box put different types of items:
  - Box A: All pens
  - Box B: All chocolates
  - Box C: A mix of pens, chocolates, coins
  - Box D: Empty or contains a single big object

Label the boxes as **Box 1, Box 2, Box 3, Box 4** but do **not** reveal what's inside.

Step-by-Step Activity

Step 1: Ask the class to guess what is inside each box.

Give them no hints.

This is **maximum entropy**: everyone is uncertain.

Step 2: Shake each box lightly

Some boxes make noise (Box C), some don't (Box A), some sound heavy (Box D).

Entropy reduces a bit because there's now some information available.

Step 3: Give a clue

Example clues:

- *"One box contains only one type of item."*

- *"One box is completely mixed."*

Now participants improve their guesses.

Entropy goes down again (uncertainty ↓).

Step 4: Open the boxes one by one

Reveal the contents.

When a box is opened, the entropy becomes **zero** — everyone knows exactly what is inside.

🎉 **Learning Outcome (Simple Explanation)**

Box	Contents	Type of Entropy	Real Meaning
Box A (only pens)	Pure, predictable	**Low entropy**	A pure quantum state (
Box C (mixed items)	Mixed, uncertain	**High entropy**	A mixed quantum state
Box D (one object)	Very predictable	**Low entropy**	Minimal uncertainty
Box with noisy shake	Moderate uncertainty	**Medium entropy**	Partially mixed quantum state

🖊 **Connecting Activity to Von Neumann Entropy**

- Each **box = quantum state ρ**
- The **variety of items = eigenvalues (λ)**
  More variety → more uncertainty → higher entropy
- Opening the box = measuring the state
  Measurement collapses uncertainty → entropy becomes zero

Von Neumann entropy measures exactly this:
"How mixed or uncertain the state is before you open the box."

Calculate the von Neumann entropy S(ρ) for the three density matrices.

The question: **Calculate the von Neumann entropy S(ρ) for the three density matrices.**

The formula we must use:

$$S(\rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

where **λ_i are the eigenvalues of ρ.**

☑ Matrix (11.41)

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

Eigenvalues

This is already diagonal → eigenvalues are:

$$\lambda_1 = 1, \quad \lambda_2 = 0$$

Entropy

$$S(\rho) = -[1 \log_2 1 + 0 \log_2 0]$$

We define $0 \log 0 = 0$.

$$S(\rho) = -[1 \cdot 0 + 0] = 0$$

✔ **Answer:**

$$\boxed{S(\rho) = 0}$$

This makes sense because it's a **pure state.**

☑ Matrix (11.42)

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

Eigenvalues

This is a projector onto $|+\rangle$.
The eigenvalues are:

$$\lambda_1 = 1, \quad \lambda_2 = 0$$

(because the matrix is rank-1)

Entropy

$$S = -[1 \log_2 1 + 0 \log_2 0] = 0$$

✔ **Answer:**

$$\boxed{S(\rho) = 0}$$

Again a **pure state.**

☑ Matrix (11.43)

$$\rho = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

This is the density matrix for the equally weighted superposition:

$$|\psi\rangle = \frac{1}{\sqrt{3}}(1,1,1)$$

Eigenvalues

A 3×3 all-ones matrix has:

- One eigenvalue = 3
- Two eigenvalues = 0

Since we multiply by $1/3$, eigenvalues become:

$$\lambda_1 = 1, \quad \lambda_2 = 0, \quad \lambda_3 = 0$$

Entropy

$$S(\rho) = -[1\log_2 1 + 0\log_2 0 + 0\log_2 0] = 0$$

✔ **Answer:**

$$\boxed{S(\rho) = 0}$$

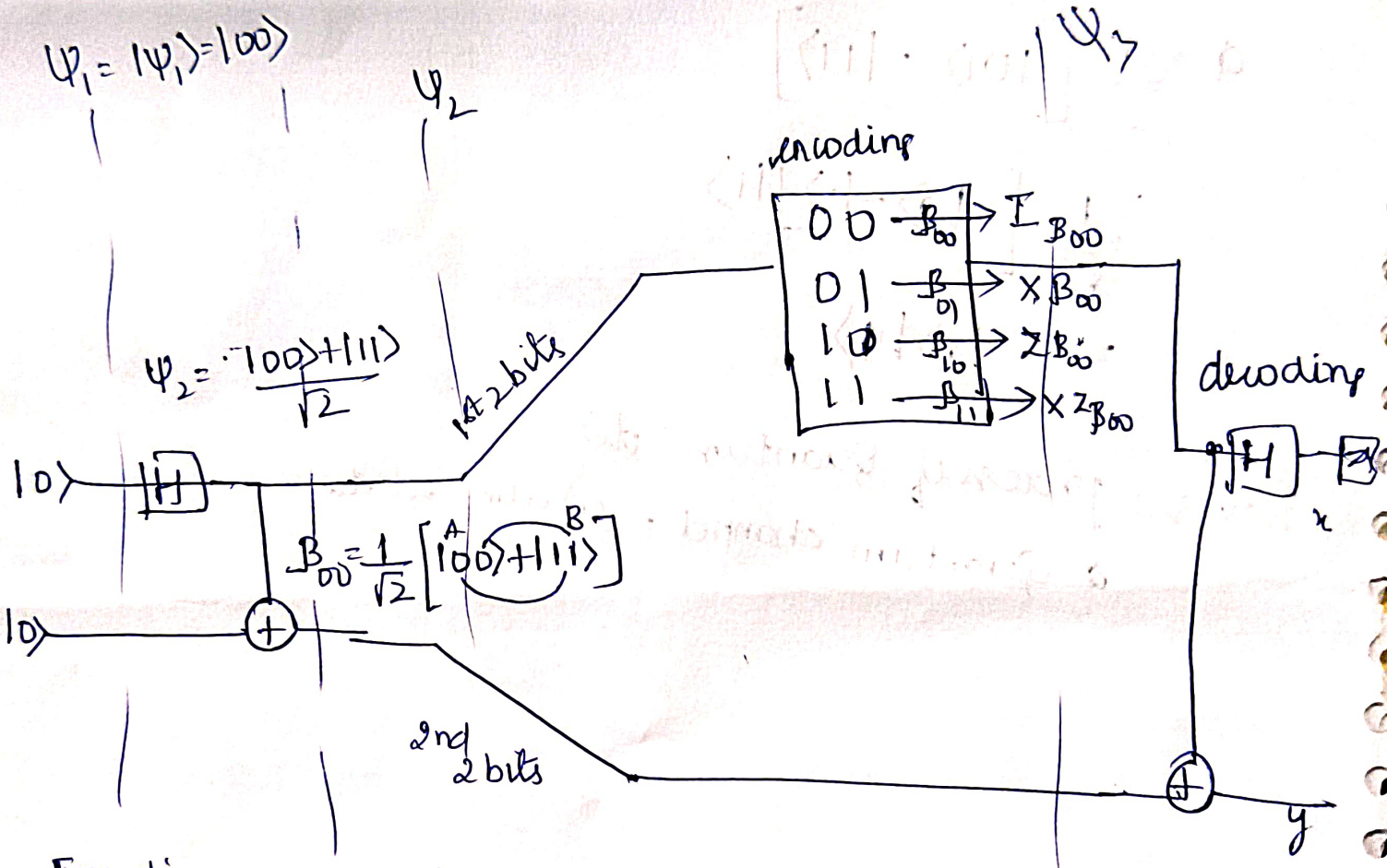
This is also a **pure state** in 3D Hilbert space.

Quantum Super dense coding

→ Reverse process of Quantum teleportation

→ Transmit 2 bits of classical information using 1 bit of Quantum information

→ Quantum information protocol



Encoding

ψ_1

ket 01

00	$-I \otimes I$
01	$-X \otimes I$
10	$-Z \otimes I$
11	$-XZ \otimes I$

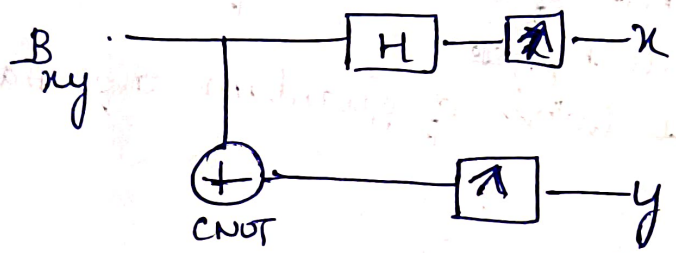
Decoding process of B

$$B_{00} = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] \xrightarrow{CX} \frac{1}{\sqrt{2}}[|00\rangle + |10\rangle]$$

$$B_{01} = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle] \xrightarrow{CX} \frac{1}{\sqrt{2}}[|01\rangle + |11\rangle] \xrightarrow{H}$$

$$B_{10} = \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle] \xrightarrow{CX} \frac{1}{\sqrt{2}}[|00\rangle - |10\rangle] \xrightarrow{H}$$

$$B_{11} = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle] \xrightarrow{CX} \frac{1}{\sqrt{2}}[|01\rangle - |11\rangle] \xrightarrow{H}$$



Apply CNOT

A) $\frac{1}{\sqrt{2}}[|00\rangle + |10\rangle]$

↓ can be

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

↓

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

$H|-\rangle = |1\rangle$

$= \frac{1}{\sqrt{2}}\boxed{[|0\rangle|0\rangle]}$ Received classical

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

B) $= \frac{1}{\sqrt{2}}|01\rangle + |11\rangle]$

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

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

$$= \frac{1}{\sqrt{2}}\left[|00\rangle - |10\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]|0\rangle$$

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

$$a = \frac{1}{\sqrt{2}}\left[|01\rangle - |11\rangle\right]$$

$$= \frac{1}{\sqrt{2}}\left[|0\rangle - |1\rangle\right]|1\rangle$$

$$= |1\rangle|1\rangle .$$

Reverse process of Quantum ite
& Quantum channel → encoding states