Qubit. (Lec 3).

- pure state (classical state)
  - i) probability of 1 is 1
  - ii) " " 0 is 0

  or

  - i) " " 1 is 0
  - ii) " " 0 is 1

- superposition (Quantum state)
  - i) probability of 1 is p. , $p < 1$
  - ii) " " 0 is $1-p$

Definition :-

unit vector

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

→ where $\alpha, \beta \in$ set of complex no's.

α, β are amplitude

$|\alpha|^2 + |\beta|^2 = 1$ (Normalization constraint)

$|\alpha|^2 = \alpha^* \alpha$ → $|\beta|^2 = \beta^* \beta$

α^* ↓ conjugate of α

Prob. of measuring 0 = $|\alpha|^2$

" " " 1 = $|\beta|^2$

Qubits examples :-

i) $|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle - \sqrt{\frac{2}{3}}|1\rangle$ → valid Qubit

$$\left|\frac{1}{\sqrt{3}}\right|^2 + \left|-\sqrt{\frac{2}{3}}\right|^2$$

$$= \frac{-i}{\sqrt{3}} \times \frac{i}{\sqrt{3}} + \left(-\sqrt{\frac{2}{3}}\right)\left(-\sqrt{\frac{2}{3}}\right)$$

$\frac{1}{3} + \frac{2}{3} = 1$ → so, valid Qubit

→ superposition state

$\frac{1}{3}$ ↓ probability of 0 is $\frac{1}{3}$

$\frac{2}{3}$ ↓ probability of 1 is $\frac{2}{3}$

ii) $|\psi\rangle = |1\rangle$ → valid Qubit

↓

It is in pure state, since probability of 1 is 1 and of 0 is 0.

$\alpha = -1 \quad \beta = 0$

iii) $|\psi\rangle = -|0\rangle$ → Valid, pure state, with probability of 0 is 1

iv) $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

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

iv) $|\psi\rangle = \frac{i}{\sqrt{7}}|00\rangle + \frac{2}{\sqrt{7}}|10\rangle + \sqrt{\frac{2}{7}}|11\rangle$ → valid qubit.

$\left|\frac{i}{\sqrt{7}}\right|^2 + \left|\frac{2}{\sqrt{7}}\right|^2 + \left|\sqrt{\frac{2}{7}}\right|^2$

$\frac{1}{7} + \frac{4}{7} + \frac{2}{7} = 1$ → valid.

probability of 00 is $\frac{1}{7}$

probability of 11 is $\frac{2}{7}$

Qubits	(M) prob	resultant state / new state
1) $\frac{i}{\sqrt{7}}\|00\rangle + \frac{2}{\sqrt{7}}\|10\rangle + \sqrt{\frac{2}{7}}\|11\rangle$	$00 \to \frac{1}{7}$, $11 \to \frac{2}{7}$ $01 \to 0$ $10 \to 4/7$	$00 \to \|00\rangle$ $10 \to \|10\rangle$ $11 \to \|11\rangle$
2) $\|00\rangle$	$00 \to 1$	$\|00\rangle$
3) $\|00\rangle$	$00 \to 1$	$\|00\rangle$

S → (m) → P

After measurement, we go into pure state from superposition state

only first qubit	
$1 \rightarrow \left\lvert\frac{2}{\sqrt{7}}\right\rvert^2 + \left\lvert\frac{\sqrt{5}}{7}\right\rvert^2$ $= 4/7 + 2/7 = 6/7$	$\frac{2}{\sqrt{7}}\lvert 10\rangle + \sqrt{\frac{2}{7}}\lvert$ $\rightarrow \sqrt{\frac{6}{7}}$
$0 \rightarrow \left\lvert\frac{1}{\sqrt{7}}\right\rvert^2 = 1/7.$	
only second qubit	
$1 \rightarrow \left\lvert\frac{2}{\sqrt{7}}\right\rvert^2 = \frac{2}{7}$	
$0 \rightarrow \left\lvert\frac{1}{\sqrt{7}}\right\rvert^2 + \left\lvert\frac{2}{\sqrt{7}}\right\rvert^2$ $= \frac{1}{7} + \frac{4}{7} = \frac{5}{7}.$	

For first qubit :-

prob of $1 = 6/7$

" " $0 = 1/7$, $= 6/7 + 1/7 = 1.$

For second qubit.

prob. of $1 = \frac{2}{7}$,

" " $0 = 5/7$, $2/7 + 5/7 = 7/7 = 1.$

Imp Normalize, and sum of probabilities should be 1.

$$\frac{\sqrt{7}}{\sqrt{6}} \times \frac{2}{\sqrt{7}} |10\rangle + \frac{\sqrt{2}}{\sqrt{6}} \times \frac{\sqrt{2}}{\sqrt{2}} |11\rangle$$

$$= \frac{2}{\sqrt{6}} |10\rangle + \frac{\sqrt{2}}{\sqrt{6}} |11\rangle$$

$$= \left(\frac{2}{\sqrt{6}}\right)^2 + \left(\frac{\sqrt{2}}{\sqrt{6}}\right)^2 = 1.$$

→ For resultant, divide orig qubits with their magnitude

$$\rightarrow \frac{\frac{i}{\sqrt{7}} |00\rangle + \frac{2}{\sqrt{7}} |10\rangle}{\sqrt{\frac{5}{7}}} = \frac{\frac{1}{\sqrt{5}} |00\rangle + \frac{2}{\sqrt{5}} |10\rangle}{}$$

(LEC 4) Equal Superposition

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

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

1-qubit

$$\frac{1}{2} |00\rangle + \frac{1}{2} |10\rangle + \frac{1}{2} |01\rangle + \frac{1}{2} |11\rangle$$

2 qubit

$\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\}$ 2D

In last lecture, we did measurements in standard basis i.e for 1st qubit $\{|0\rangle, |1\rangle\}$, we can calculate in non-standard basis

lets take a look on orthonormal form

orthogonal vectors which are normalized

$$\begin{pmatrix}3\\4\end{pmatrix} = 3|0\rangle + 4|1\rangle$$

Now, normalized vector is

$$|\psi\rangle \begin{pmatrix}3/5\\4/5\end{pmatrix} = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$$

magnitude $\sqrt{\langle\psi|\psi\rangle} = \sqrt{3^2+4^2} = 5$

Now, we have orthonormal basis

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

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

$|+\rangle$, $|-\rangle$ unit vectors normalize

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

Now, we can measure in +,- basis?

we have to rewrite

$$|\psi\rangle = \langle\psi|+\rangle|+\rangle + \langle\psi|-\rangle|-\rangle$$

$$|\psi\rangle = \langle\psi|\alpha\rangle|\alpha\rangle + \langle\psi|\beta\rangle|\beta\rangle$$

→ Inner product of orthogonal vectors is zero $\langle +|- \rangle = 0$.

∴ prob. of + equals $|\langle \psi|+\rangle|^2$

∴ " " − equals $|\langle \psi|-\rangle|^2$

$$|\psi\rangle = \left(\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right)\left(\frac{|0\rangle + |1\rangle}{2}\right)|+\rangle$$

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

By solving

$$|\psi\rangle = \left(\frac{1}{\sqrt{6}} + \sqrt{\frac{2}{6}}\right)|+\rangle + \left(\frac{1}{\sqrt{6}} - \sqrt{\frac{2}{6}}\right)|-\rangle$$

Now, to check of valid qubit

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

$$= \left(\frac{1+\sqrt{2}}{\sqrt{6}}\right)^2 + \left(\frac{1-\sqrt{2}}{\sqrt{6}}\right)$$

$$= \frac{1+2+2\sqrt{2}+1+2-\sqrt{2}(2)}{6}$$

$= 6/6 = 1$ Proved it is valid

$|-\rangle$

★ Inner product of $|+\rangle$ with itself is 1

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

$\langle 0|0\rangle = 1$

$\langle 1|1\rangle = 1$

$\langle 0|1\rangle = 0$

$\langle 1|0\rangle = 0$

Quantum Gates

→ Standard basis.

$|\psi\rangle = |0\rangle$

prob. of (M) 0 $= |1|^2 = 1$

" " (M) 1 $= 0$

→ Hadamard basis :-

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

Prob of (M) $|+\rangle$

$= |\langle +|+\rangle|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

$\downarrow$

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

$= \frac{1}{\sqrt{2}}$

$|\psi\rangle = \left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)|+\rangle + \left(\frac{1}{\sqrt{6}} + \frac{1}{\sqrt{3}}\right)|-$

Standard.

Hadamard basis

Prob of (M) $+ = \left|\left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\right|^2$

$$= \frac{1}{6} + \frac{1}{3} - \frac{2}{\sqrt{6}\sqrt{3}} = \frac{3 - 2\sqrt{2}}{6}$$

Prob of (M) $|-\rangle = 1 - \left(\frac{3-2\sqrt{2}}{6}\right)$

// // $= \frac{3+2\sqrt{2}}{6}$

Hamdard

basis: $\{|0\rangle, |1\rangle\}$

prob of (m) + (0) $= |\langle +|0\rangle|^2$

$$\langle +|0\rangle = \left[\left[\left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\langle +| + \left(\frac{1}{\sqrt{6}} + \frac{1}{\sqrt{3}}\right)\langle -|\right]|0\rangle\right]$$

$$= \left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\langle +|0\rangle + \left(\frac{1}{\sqrt{6}} + \frac{1}{\sqrt{3}}\right)\langle -|0\rangle$$

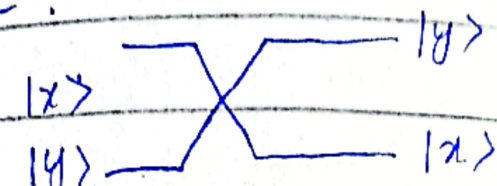
$\langle +|0\rangle = \frac{1}{\sqrt{2}}$

$$= \left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\left(\frac{1}{\sqrt{2}}\right) + \left(\frac{1}{\sqrt{6}} + \frac{1}{\sqrt{3}}\right)\left(\frac{1}{\sqrt{2}}\right)$$

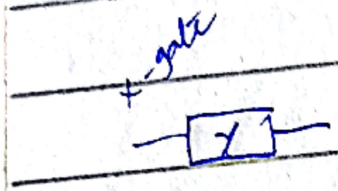
$$= \frac{1}{\sqrt{3}} \longrightarrow \left(\frac{1}{\sqrt{3}}\right)^2$$

Prob of (m) $|1\rangle = 1 - \frac{1}{3} = \frac{2}{3}$

Swap Gate:



1-gate



Hamadard gate

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

SWAP $(\alpha|01\rangle + \beta|10\rangle)$

$= \alpha|10\rangle + \beta|01\rangle$

CNOT

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

control bit — apply not on this

CNOT $|10\rangle = |11\rangle$

CNOT $|01\rangle = |01\rangle$

CNOT $|11\rangle = |10\rangle$

control bit should be 1

CZ $|01\rangle = |01\rangle$ change sign of 1 place at pos of second bit

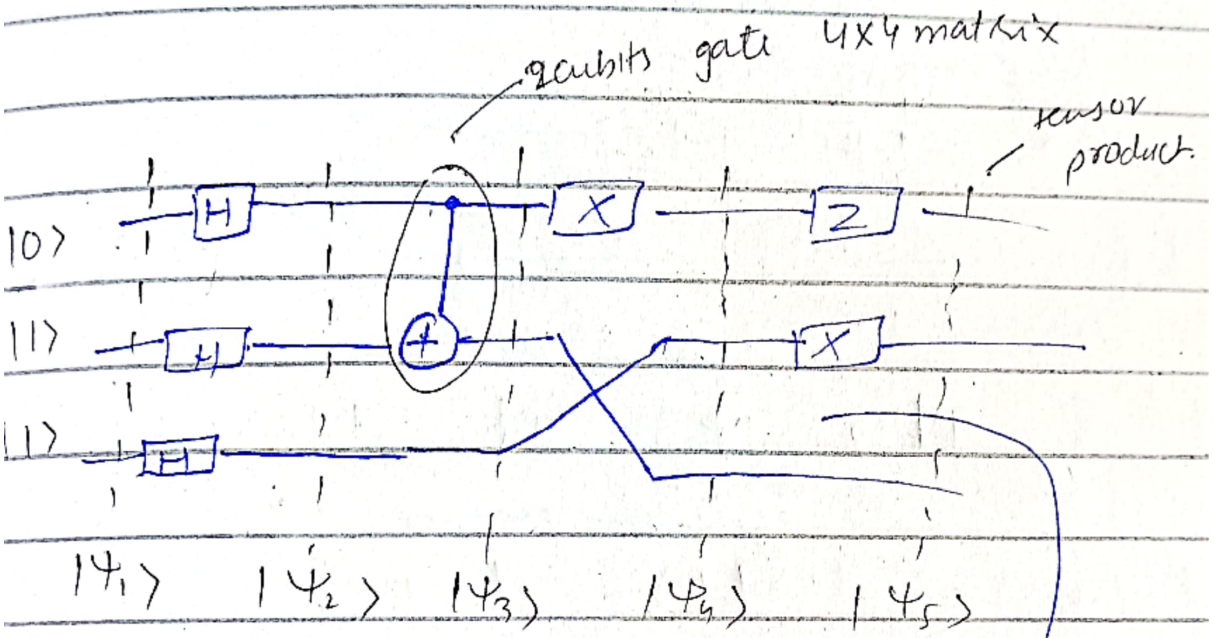
CZ $|11\rangle = -|11\rangle$

CZ $|10\rangle = |10\rangle$

For hermitian gates, we don't need to take their conjugate transpose

$$Z|0\rangle = |0\rangle \quad , \quad Z|1\rangle = -|1\rangle$$

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



since no gate, so identity gate is present

8x8 matrix

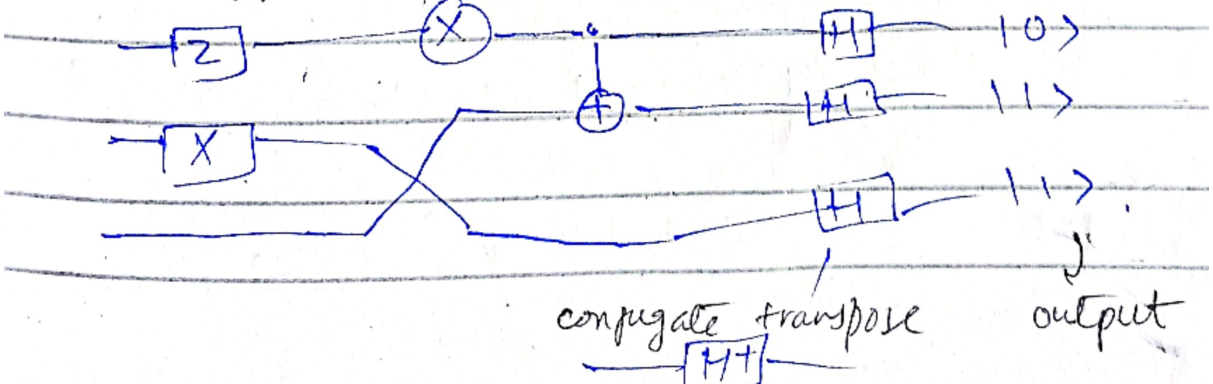
Circuit matrix 2x2 4x4

$$[(Z \otimes X \otimes I)(X \otimes \text{Swap})(\text{cnot} \otimes I)\cdot(H^{\otimes 3})]$$

4x4 2x2

$|011\rangle \rightarrow$ input

Reverse of above circuit.



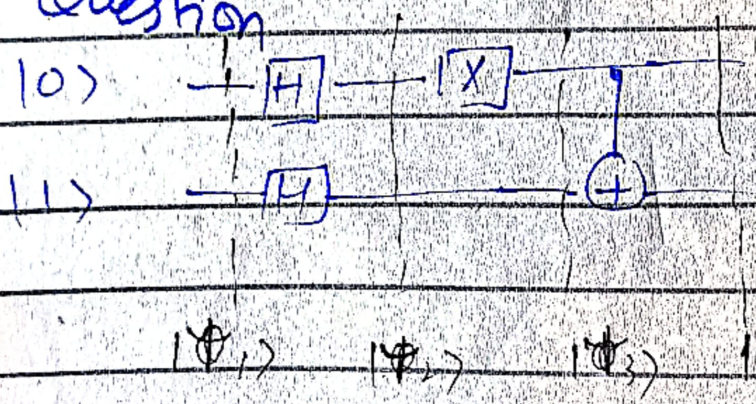
Q1 what will be the output ?

Q2 Create unitary matrix of circuit.

Q3 Create reverse circuit.

Q4 create unitary matrix of reverse circuit.

Question



tensor product

$|\Psi_1\rangle = |0\rangle|1\rangle = |01\rangle$

$|\Psi_2\rangle = H|0\rangle \otimes H|1\rangle$

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

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

$|\Psi_3\rangle = X|\Psi_2\rangle$

not gate on only first qubit

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

$|\Psi_4\rangle = CNOT\,|\Psi_3\rangle$

output of circuit

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

(1)

Finding output using matrices (long method)

$$|\psi_1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

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

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad (1)$$

$$= \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = |\psi_2\rangle$$

Braket notation of same que should be equal to this

tensor product

$|\psi_3\rangle$ = First ~~multiply~~ X with Identity to form 4 X 4

can't multiply X with $|\psi_2\rangle$ because X is 2x2 matrix, and $|\psi_2\rangle$ is 4 x 1

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

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

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

$$|\psi_3\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

$\xrightarrow{CNOT}$

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

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

→ If we write bracket notation of this it is equal to (1)

Q2: Unitary matrix

3 × 2 × 1

CNOT $X \otimes I$ $H^{\otimes 2}$

$(AB)^T = B^T A^T$

Q4: $(3 \times 2 \times 1)^T = (1^T \times 2^T \times 3^T)$

Foundation for Advancement of Science & Technology

Qubits	M. Prob	New State
$\frac{i}{\sqrt{7}}\|00\rangle + \frac{2}{\sqrt{7}}\|10\rangle + \sqrt{\frac{2}{7}}\|11\rangle$	$00 \to 1/7$ $\quad 01 \to 0$ $10 \to 4/7$ $\quad 11 \to 2/7$	$00 \longrightarrow \|00\rangle$ $10 \longrightarrow \|10\rangle$ $11 \longrightarrow \|11\rangle$
$\|00\rangle$ $\|00\rangle$	$00 \to 1$	$\|00\rangle$
$\frac{i}{\sqrt{7}}\|00\rangle + \frac{2}{\sqrt{7}}\|10\rangle + \sqrt{\frac{2}{7}}\|11\rangle$	Only first bit $1 \to \left\|\frac{2}{\sqrt{7}}\right\|^2 + \left\|\sqrt{\frac{2}{7}}\right\|^2 = 6/7$ $0 \to \left\|\frac{i}{\sqrt{7}}\right\|^2 = \frac{1}{7}$	$\frac{\frac{2}{\sqrt{7}}\|10\rangle + \sqrt{\frac{2}{7}}\|11\rangle}{\sqrt{\frac{6}{7}}}$ $\frac{2}{\sqrt{6}}\|10\rangle + \sqrt{\frac{2}{6}}\|11\rangle$ $\frac{i/\sqrt{7}\|00\rangle}{1/\sqrt{7}} = i\|00\rangle$
	Only Second Qubit $1 \to \left\|\sqrt{\frac{2}{7}}\right\|^2 = \frac{2}{7}$	$\frac{\sqrt{\frac{2}{7}}\|11\rangle}{\sqrt{2/7}} = \|11\rangle$
	$0 \to \left\|\frac{i}{\sqrt{7}}\right\|^2 + \left\|\frac{2}{\sqrt{7}}\right\|^2$ $= \frac{1}{7} + \frac{4}{7} = \frac{5}{7}$	$\frac{\frac{i}{\sqrt{7}}\|00\rangle + \frac{2}{\sqrt{7}}\|10\rangle}{\sqrt{5/7}}$ $\frac{i}{\sqrt{5}}\|00\rangle + \frac{2}{\sqrt{5}}\|10\rangle$

1-2-24 Equal Superposition

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

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

} 1-qubit

$\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle$ } 2-qubit

Foundation for Advancement of Science & Technology

ψ, ϕ are orthogonal if $\langle\psi|\phi\rangle = 0$.

In last lecture we did measurement in standard basis i.e for 1st qubit $\{|0\rangle, |1\rangle\}$. 2 qubit $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. We can do in basis as well but it should be in orthonormal form.

Now what is orthonormal formal:

Let we have a vector: $\begin{pmatrix} 3 \\ 4 \end{pmatrix} = 3|0\rangle + 4|1\rangle$

$\sqrt{\langle\psi|\psi\rangle}$ is magnitude $\Rightarrow \sqrt{3^2+4^2} = 5$

Now, normalized vector is: $|\psi'\rangle = \begin{pmatrix} 3/5 \\ 4/5 \end{pmatrix} = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$

Now we have an orthonormal basis $\{|+\rangle, |-\rangle\}$

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

Now can we measure in +,- basis? We have to rewrite: $|\psi\rangle = \langle\psi|+\rangle|+\rangle + \langle\psi|-\rangle|-\rangle$

$\therefore$ prob of + equals $|\langle\psi|+\rangle|^2$, - equals $|\langle\psi|-\rangle|^2$.

$$|\psi\rangle = \left(\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|+\rangle + \left(\frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|-\rangle$$

By solving

$$|\psi\rangle = \left(\frac{1}{\sqrt{6}} + \sqrt{\frac{2}{6}}\right)|+\rangle + \left(\frac{1}{\sqrt{6}} - \sqrt{\frac{2}{6}}\right)|-\rangle$$

Now to check if valid qubit $(|\alpha|^2 + |\beta|^2 = 1)$

$$\left(\frac{1+\sqrt{2}}{\sqrt{6}}\right)^2 + \left(\frac{1-\sqrt{2}}{\sqrt{6}}\right)$$

$$= \frac{1+2+2\sqrt{2}+1+2-\sqrt{2}(2)}{6} = \frac{6}{6} = 1$$ (Proved its valid qubit)

Quiz 2

Foundation for Advancement of Science & Technology

Quantum Gates

Qubits are vectors; Quantum gates are matrices.

★ This should be such matrices which preserve the norm i.e after matrix multiplication sum of probabilities should remain 1.

$\Rightarrow U|\psi\rangle = |\phi\rangle$ U is quantum gate (matrix)

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

$= \sqrt{(U|\psi\rangle)^\dagger (U|\psi\rangle)} = \sqrt{\langle\psi|U^\dagger U|\psi\rangle}$

So, for $\sqrt{\langle\phi|\phi\rangle} = \sqrt{\langle\psi|\psi\rangle}$ $U^\dagger U = I$.

So, quantum gates must be unitry matrices ($U^\dagger U = U U^\dagger = I$).

The raws, cols of unitry matrix make orthonormal basis. Cols proof in class, row proof do by yourself.

For cols prove $U^\dagger U = I$, for raw prove $U U^\dagger = I$.

For cols: $U^\dagger U = I$.

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} a_{11}^* & a_{21}^* & a_{31}^* \\ a_{12}^* & a_{22}^* & a_{32}^* \\ a_{13}^* & a_{23}^* & a_{33}^* \end{pmatrix} \begin{matrix} \leftarrow C_1^\dagger \\ \leftarrow C_2^\dagger \\ \leftarrow C_3^\dagger \end{matrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

U $\qquad$ $U^\dagger$

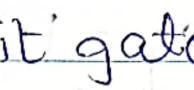
$$\begin{pmatrix} C_1^\dagger \cdot C_1 & C_1^\dagger \cdot C_2 & C_1^\dagger C_3 \\ C_2^\dagger \cdot C_1 & C_2^\dagger \cdot C_2 & C_2^\dagger \cdot C_3 \\ C_3^\dagger \cdot C_1 & C_3^\dagger \cdot C_2 & C_3^\dagger \cdot C_3 \end{pmatrix} = \begin{pmatrix} \langle C_1|C_1\rangle & \langle C_1|C_2\rangle & \langle C_1|C_3\rangle \\ \langle C_2|C_1\rangle & \langle C_2|C_2\rangle & \langle C_2|C_3\rangle \\ \langle C_3|C_1\rangle & \langle C_3|C_2\rangle & \langle C_3|C_3\rangle \end{pmatrix}$$

as $\langle C_1|C_1\rangle, \langle C_2|C_2\rangle, \langle C_3|C_3\rangle$ are equal to 1, so C_1, C_2, C_3 are orthogonal

So, columns are part of orthonomal basis.

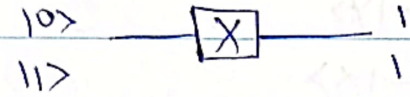
All gates are reversible. To reverse the result use $U^\dagger$. But if U is hermitian i.e $U^\dagger = U$. Then dont need conjugate transpose of unitry matrix.

Now, some about Quantum Gates.

Pauli-X Gate: Single qubit gate : 

NOT Gate

So, unitary matrix shall be 2x2 (one bit $2^1=2$)



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

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

★ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is unitary matrix.

$X|0\rangle = |1\rangle$ (proved)

Pauli-Z Gate: Single Qubit Gate 

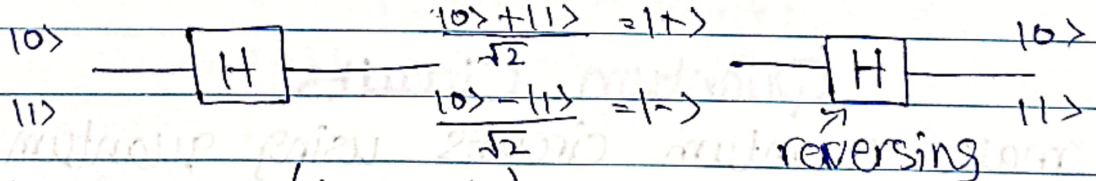
$Z|0\rangle = |0\rangle$ but $Z|1\rangle = -|1\rangle$

Unitary matrix $\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

Z $|1\rangle$

Hadamard Gate: Single Qubit Gate (most widely used → imp as well) takes $|0\rangle$, $|1\rangle$ and converts into equal superposition (+,-).



Unity Matrix $\Rightarrow \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Now practice, $H|-\rangle = |1\rangle \Rightarrow \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

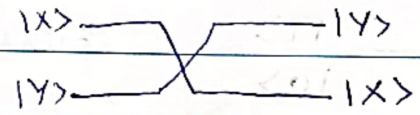
$$= \frac{1}{2}\begin{pmatrix} 1\times1 + 1\times(-1) \\ 1\times1 + (-1)(-1) \end{pmatrix}$$

Foundation for Advancement of Science & Technology

$= \frac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$ (Hence, proved)

Election holidays L-5,6 L-7

Swap Gate



* it is 2-qubit gate with matrix $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Example: $SWAP(\alpha|01\rangle + \beta|10\rangle)$
$= \alpha|10\rangle + \beta|01\rangle$

Control-NOT

$CNOT|10\rangle = |11\rangle$
$CNOT|01\rangle = |01\rangle$

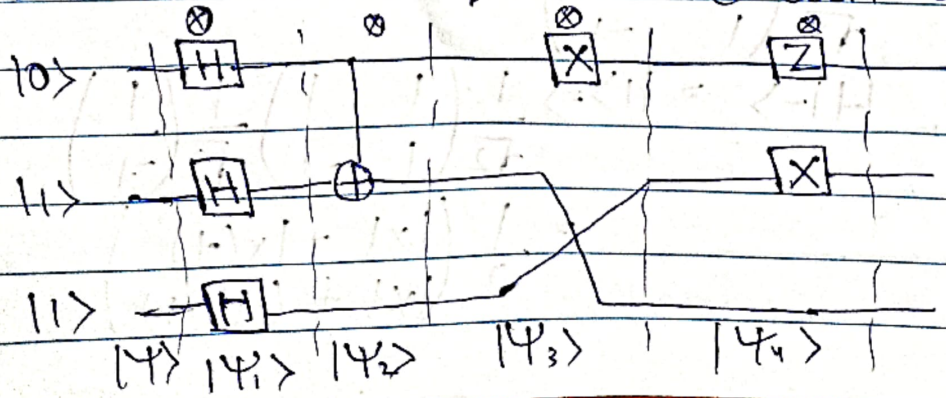
changes second bit, but only when first bit is '1'. Eg:
$CNOT|11\rangle = |10\rangle$

$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ ← NOT gate

* we can make other control gates such as C-OR, C-Hadamard, C-Z but first bit should be 1.
Examples: $CZ|01\rangle = |01\rangle$, $CZ|11\rangle = -|11\rangle$, $CZ|10\rangle = |10\rangle$

Quantum Circuits

* we make quantum circuits using quantum gates.
Suppose we have a quantum circuit of 3 qubits:



Foundation for Advancement of Science & Technology

(1)

So we can do $|H|0\rangle \otimes |H|1\rangle \otimes |H|1\rangle$ or $H^{\otimes 3}|011\rangle$

$(CNOT \otimes I(H^{\otimes 3}|011\rangle) \Rightarrow X \otimes SWAP(CNOT \otimes I(H^{\otimes 3}|011\rangle))$

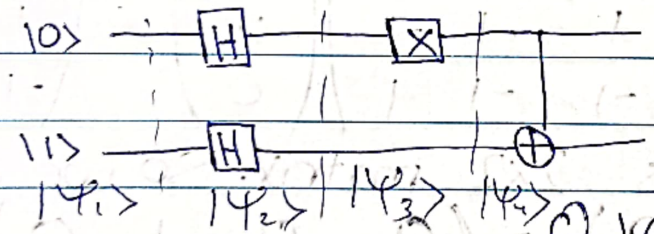
Then complete it. Main thing is that we have to make a matrix of the complete circuit. Complete circuit is:

$$[(Z \otimes X \otimes I) \cdot (X \otimes SWAP) \cdot (CNOT \otimes I) \cdot (H^{\otimes 3})] \cdot |011\rangle$$

This is 8x8 matrix, Lets do a 4x4 one

*To, reverse the gate:

Lets do a 4x4 matrix for a circuit:



Q1) What is the output

Q2) What is its unitry matrix

Q3) Create its reverse circuit.

Q4) Create unitry matrix of " "

We can get output using matrices or braket notation. First doing using braket notation:

$|\psi_1\rangle = |0\rangle \otimes |1\rangle = |01\rangle$

$|\psi_2\rangle = H|0\rangle \otimes H|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

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

$|\psi_3\rangle = X|\psi_2\rangle = \frac{1}{2}(|10\rangle - |11\rangle + |00\rangle - |01\rangle)$

Foundation for Advancement of Science & Technology

$$|\psi_4\rangle = CNOT\,|\psi_3\rangle = \frac{1}{2}\left(|111\rangle - |110\rangle + |100\rangle - |101\rangle\right)$$

This output of circuit (Ans. of Q_1)

Now using matrices:

$$|\psi_1\rangle = |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

Now before $|\psi_2\rangle$, finding $H^{\otimes 2}$.

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

$$\text{Now, } |\psi_2\rangle = H^{\otimes 2}|\psi_1\rangle = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}$$

$|\psi_3\rangle = X|\psi_2\rangle$ but X is 2×2 matrix. So we do,

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

$$|\psi_3\rangle = (X \otimes I)|\psi_2\rangle = \begin{pmatrix}0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{pmatrix}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}\cdot\frac{1}{2} = \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}\frac{1}{2}$$

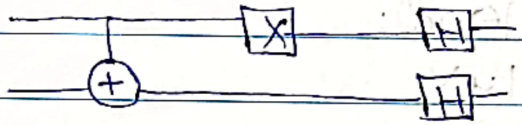
Foundation for Advancement of Science & Technology

$$|\psi_4\rangle = CNOT\,|\psi_3\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

Verify, $|\psi_4\rangle$ from braket notation is same as the answer from matrices. Yes it is same (check if not clear) (Ans. of Q_1) ↗

Now, making unitry matrix: first we apply $H^{\otimes 2}$, then $X \otimes I$ then CNOT. So, answer shall be $H^{\otimes 2} \times (X \otimes I) \times CNOT$ (Do by yourself). (Ans. Q_2)

Ans(Q_3)



Ans(Q_4) Conjugate transpose of Ans(Q_2) OR we see Ans(Q_3) and ans becomes $CNOT^{\dagger} \times X^{\dagger} \times H^{\dagger \otimes 2}$ here CNOT, X, $H^{\otimes 2}$ are hermitian so it remains same as At original matrices ($CNOT \times X \times H^{\otimes 2}$).

15-2-24 L-8

We try to generalize Hadamard gate as $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. So we make general expression: $H|x\rangle = \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}}$ where $x = 0, 1$

also $H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x \cdot y} |y\rangle$ $\quad x \cdot y = x$ AND y

Example => $x=0$

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

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

This formula can be used for bigger numbers too.

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

$x\cdot y = x_1 y_1 + x_2 y_2 + \cdots x_n y_n$ consider them decimal values

here $\sum_{y=0}^{2^n-1}$ is equal to $\sum_{y=\{0,1\}^n}$ ← it means y is made of 0,1 with n length.

So, $\sum_{y=\{0,1\}^2}$ = 00, 01, 10, 11 (in binary)

and $\sum_{y=0}^{2^2-1}$ = 0, 1, 2, 3 (in decimal)

Now, example to understand:

$$H^{\otimes 2}|01\rangle = \frac{1}{\sqrt{2^2}} \sum_{y=0}^{2^2-1} (-1)^{x\cdot y}|y\rangle$$

$$= \frac{1}{2}\Big[\underset{\substack{x=01\\ y=00\\ x\cdot y=0\cdot 0+1\cdot 0=0}}{(-1)^0}|00\rangle + \underset{\substack{x=01\\ y=01\\ x\cdot y=0\cdot 0+1\cdot 1=1}}{(-1)^1}|01\rangle + \underset{\substack{x=01\\ y=10\\ x\cdot y=0\cdot 1+1\cdot 0=0}}{(-1)^0}|10\rangle + \underset{\substack{x=01\\ y=11\\ x\cdot y=0\cdot 1+1\cdot 1=1}}{(-1)^1}|11\rangle\Big]$$

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

Now, $x\cdot y = x_1\cdot y_1 + x_2\cdot y_2 + \cdots + x_n\cdot y_n$ is long and boring. So, we do, by example:

$$H^{\otimes 3}|101\rangle = \frac{1}{\sqrt{2^3}}\left[|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle\right]$$

First see $|101\rangle$, skip 0 because it shall give 0; So we see first and last bit of $|y\rangle$ values.

Our new way is fast but is becomes slow if we have to calculate: $H^{\otimes 3}(|010\rangle - |011\rangle + |111\rangle)$. So do,

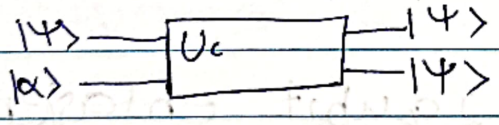
sign change ↓	000	001	010	011	100	101	110	111
010	+ (without sign change)	+	−	−	+	+	−	−
−011	+ −	− +	− +	+ −	+ −	− +	− +	+ −
111	+	−	−	+	−	+	+	−
	1	1	−1	−1	−1	+3	1	−3

$$H^{\otimes 3}(|010\rangle - |011\rangle + |111\rangle) = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle - |010\rangle - |011\rangle - |100\rangle + 3|101\rangle + |110\rangle - 3|111\rangle)$$

20-2-24 **Cloning** L-9

Let say we want to store some info in 'α' in "$\alpha|0\rangle + \beta|1\rangle$" qubit. But to make it valid qubit we need to store its inverse in $\beta(\alpha^2 + \beta^2 = 1)$.

So, to extract info from α we use a cloning machine, because in qubit we shall either get 0, 1.



we approximate the result from U_c to get almost correct value of α (approximate in billions/trillions).

No Cloning Theorem: Cannot create a unitary operator that take an arbitrary qubit and clone it. (U_c doesnot preserves inner product/norm)

$U|\alpha\rangle = |\alpha|\beta\rangle$ and $U|x\rangle = |y\rangle$

then $\langle\alpha|x\rangle = \langle\beta|y\rangle$

Foundation for Advancement of Science & Technology

Proof: $U_c|\psi\rangle|\alpha\rangle = |\psi\rangle|\psi\rangle$

$U_c|x\rangle|\alpha\rangle = |x\rangle|x\rangle$

Now check if norm preserved:

$$\underbrace{(|\psi\rangle|\alpha\rangle)^\dagger}_{a}\underbrace{(|x\rangle|\alpha\rangle)}_{x} = \underbrace{(|\psi\rangle|\psi\rangle)^\dagger}_{b}\underbrace{(|x\rangle|x\rangle)}_{y}$$

$$\underbrace{\langle\psi|x\rangle}_{\text{number}}|\alpha\rangle = \langle\psi|\underbrace{\langle\psi|x\rangle}_{\text{number}}|x\rangle$$

$\langle\psi|x\rangle\langle\alpha|\alpha\rangle = \langle\psi|x\rangle\langle\psi|x\rangle$

$\langle\psi|x\rangle = \langle\psi|x\rangle^2$

↳ Only when $\langle\psi|x\rangle = 0$ and $0 = 0^2$ (orthogonal vector)

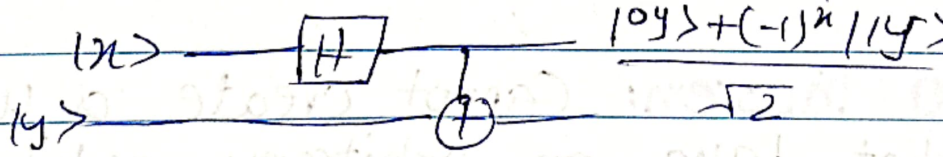
or $\langle\psi|x\rangle = 1$ " $1 = 1^2$ (same vectors)

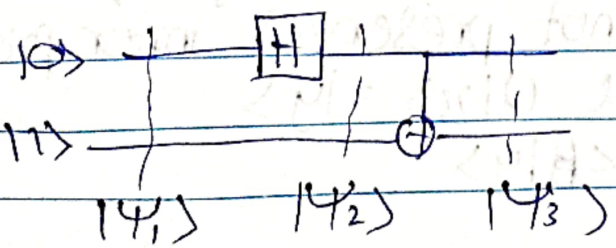
Hence proved, we cannot make a general U_c.

Entanglement

Let we have a 2 qubit register $|\psi\rangle$, it is not entangled if : $|\psi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \gamma|1\rangle)$ and measuring one, reveals other qubit

2-qubit entanglement: 2 qubit entanglement is called bell states. 3 or more qubit entanglement are called GHZ states. So, in 2-qubit:



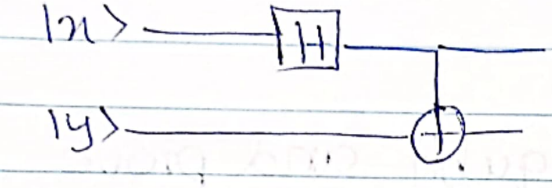


Foundation for Advancement of Science & Technology

$|\psi_1\rangle = |01\rangle$ $\quad |\psi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} |1\rangle = \frac{|01\rangle + |11\rangle}{\sqrt{2}}$

$|\psi_3\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$ ← this is a bell state.

Now, verify if we get it from the formula.



$= \frac{|0y\rangle + (-1)^x |1\bar{y}\rangle}{\sqrt{2}} = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$ (proved)

So, there are 4 bell states:

input	output
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2}$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2}$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2}$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2}$

here, if one qubit is one other is itself revealed.

Look $\frac{|00\rangle + |01\rangle}{\sqrt{2}}$ is not entangled, because first qubit is 0 in $|00\rangle$ and in $|01\rangle$ so, this is not possible. In entangled qubits (bell states) a qubit is never same in two $|\psi\rangle$'s.

Now, lets proved $(|00\rangle - |11\rangle)/\sqrt{2}$ is entangled.

Proof (by contradiction): we assume it is not entangled.

So, $\frac{|00\rangle - |11\rangle}{\sqrt{2}} = (\alpha|0\rangle + \beta|1\rangle)(x|0\rangle + y|1\rangle)$

$\frac{|00\rangle}{\sqrt{2}} \quad \frac{-|11\rangle}{\sqrt{2}} = \alpha x|00\rangle + \alpha y|01\rangle + \beta x|10\rangle + \beta y|11\rangle$

$\alpha x = \frac{1}{\sqrt{2}}$, $\alpha y = 0$, $\beta x = 0$, $\beta y = \frac{-1}{\sqrt{2}}$

Foundation for Advancement of Science & Technology

Consider $\alpha y = 0$ then either $\alpha = 0$ or $y = 0$ or $\alpha, y = 0$.
but $\alpha \neq 0$ as $\alpha x = 1/\sqrt{2}$, also, $y \neq 0$ as $\beta y = 1/\sqrt{2}$.
Hence, proved it is entangled as:
$\frac{|00\rangle - |11\rangle}{\sqrt{2}} = (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + y|1\rangle)$ is false

Now, lets take a non-entangled qubit and prove it non-entangled Take $\Rightarrow \frac{1}{2\sqrt{3}}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + y|1\rangle) =$

$\frac{1}{2\sqrt{3}}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{\sqrt{6}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle = \alpha x|00\rangle + \alpha y|01\rangle + \beta x|10\rangle + \beta y|11\rangle$

$\alpha x = \frac{1}{2\sqrt{3}}$ $\alpha y = \frac{1}{2}$ $\beta x = \frac{1}{\sqrt{6}}$ $\beta y = \frac{1}{\sqrt{2}}$

Now find values of α, β, x, y $(|\alpha|^2 + |\beta|^2 = 1 = |x|^2 + |y|^2)$

So, $\underbrace{\left(\frac{1}{2x\sqrt{3}}\right)^2}_{\alpha^2} + \underbrace{\left(\frac{1}{x\sqrt{6}}\right)^2}_{\beta^2} = 1 \Rightarrow \frac{1}{12x^2} + \frac{1}{6x^2} = 1 \Rightarrow \frac{1}{12} + \frac{1}{6} = x^2$

By solving, $x = 1/2 \Rightarrow \alpha = 1/\sqrt{3}$, $\beta = \sqrt{\frac{2}{3}}$

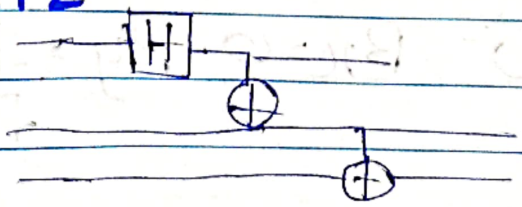
(as, $\beta x = \frac{1}{\sqrt{6}}$ so, ~~$\beta = \frac{1}{\sqrt{6}} \cdot \frac{1}{2}$~~ ≠)

$\beta y = \frac{1}{\sqrt{2}}$ so, $y = \frac{\sqrt{3}}{2}$

So, it is not entangle.

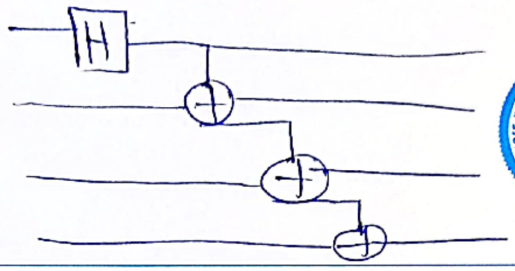
GHZ

For 3 qubit:



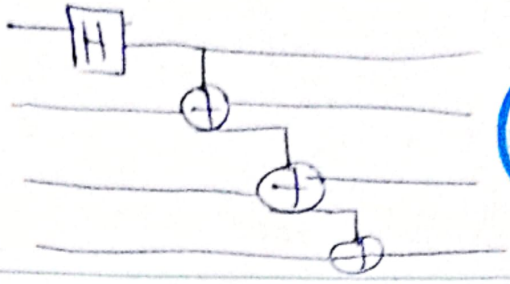
Foundation for Advancement of Science & Technology

For 4-qubit:



in 3-qubit input can only be $|000\rangle$, $|111\rangle$ in 4-qubit input can only be $|0000\rangle$, $|1111\rangle$.

For 4-qubit:



in 3-qubit, input can only be $|000\rangle$, $|111\rangle$ in 4-qubit input can only be $|0000\rangle$, $|1111\rangle$.

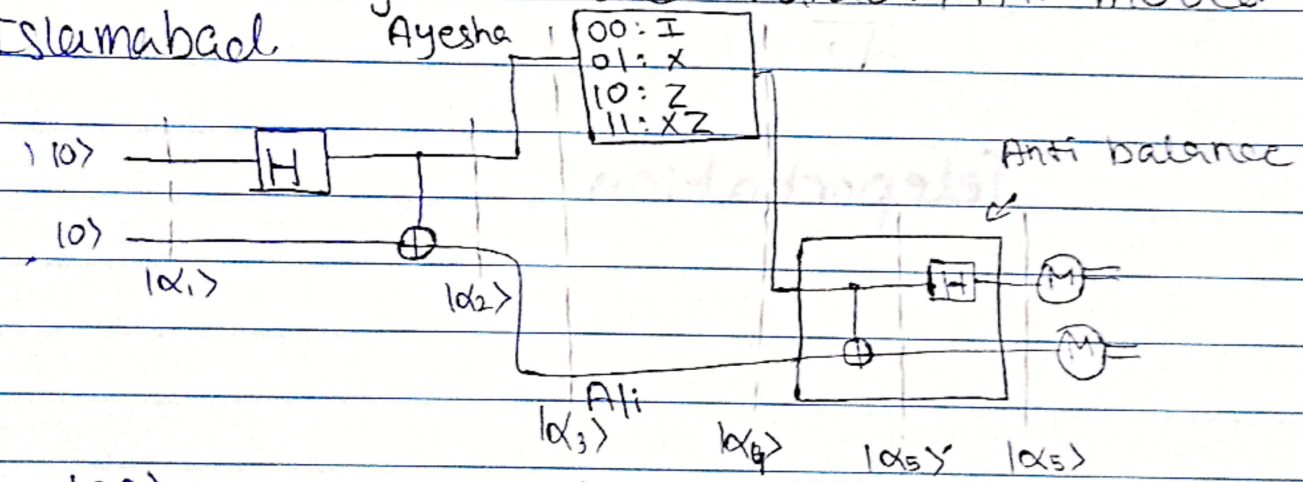
22-2-24 L-10

Superdense coding: send 2 classical bits by sending a qubit.

Quantum teleportation: You send a qubit, by sending 2 classical bits.

Superdense Coding

Ayesha and Ali worked together and made a balanced state. Ayesha moved Karachi, Ali moved to Islamabad



$|\alpha_1\rangle = |00\rangle$ $\quad |\alpha_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\alpha_3\rangle$

$|\alpha_4\rangle$ depends upon what we send i.e 00, 01, 10, 11.

Let suppose we send 10 (So apply Z gate).

$|\alpha_4\rangle = Z|\alpha_3\rangle = Z\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

Foundation for Advancement of Science & Technology

$|\alpha_5\rangle' = \frac{|00\rangle - |10\rangle}{\sqrt{2}}$ $\quad |\alpha_5\rangle = H\left(\frac{|00\rangle - |10\rangle}{\sqrt{2}}\right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle - \frac{|0\rangle - |1\rangle}{\sqrt{2}}|0\rangle$

$|\alpha_5\rangle = \frac{|00\rangle + |10\rangle - |00\rangle + |10\rangle}{\sqrt{2}\cdot\sqrt{2}} = \frac{2|10\rangle}{2} = |10\rangle$

If we have to send 11: $|\alpha_3\rangle$ shall be same.

$|\alpha_4\rangle = XZ|\alpha_3\rangle = X\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \frac{|01\rangle + |10\rangle}{\sqrt{2}} = Z\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right)$

$|\alpha_4\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ $\quad |\alpha_5\rangle' = \frac{|01\rangle - |11\rangle}{\sqrt{2}}$

$|\alpha_5\rangle = \frac{\frac{|0\rangle + |1\rangle}{\sqrt{2}}|1\rangle - \frac{|0\rangle + |1\rangle}{\sqrt{2}}|1\rangle}{\sqrt{2}} = |11\rangle$

Teleportation

Classical to Quantum Deutsch Josza Algo

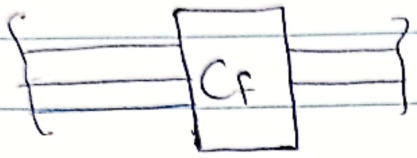
Foundation for Advancement of Science & Technology

5-3-24

Classical to Quantum

L-11

$f: \{0,1\}^n \longrightarrow \{0,1\}^m$ classical func.



but quantum circuits are reversible, this circuit is not.

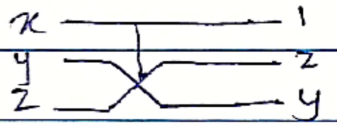
So, first we make it reversible.

- Universal classical Gate (By which we can make any gate)

1) Not (reversible), AND (not reversible) (can make any gate from these two)

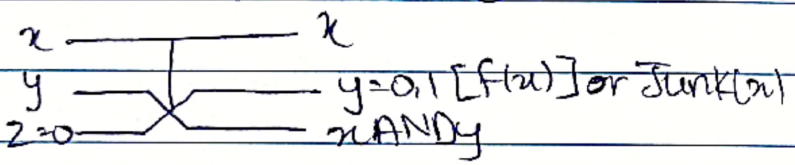
We redesign AND Gate to make it reversible.

So, we use controlled-SWAP.



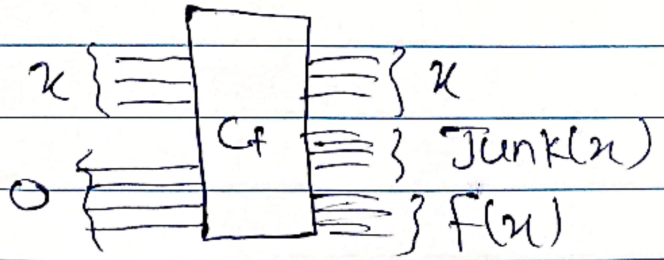
← it is also a quantum gate.

We make AND from C-SWAP. Let we put z=0:

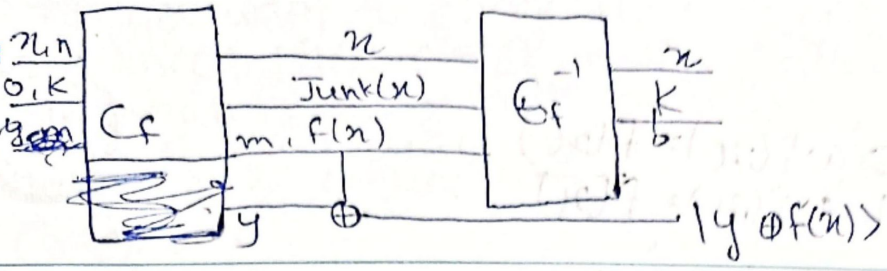


x	y	
0	0	z=0
0	1	z=0
1	0	y=0
1	1	y=1

We, use NOT and C-SWAP in the classical func we had to make:



it IS a reversible circuit, but Junck(x) can get entangled with f(x), but we want to not have Junck(x).



The quantum circuit now is: $|x\rangle$ (n) $|y\rangle$ (m) $\rightarrow$ Q_f $\rightarrow$ $|x\rangle$ (n), $|f(x) \oplus y\rangle$ (m)

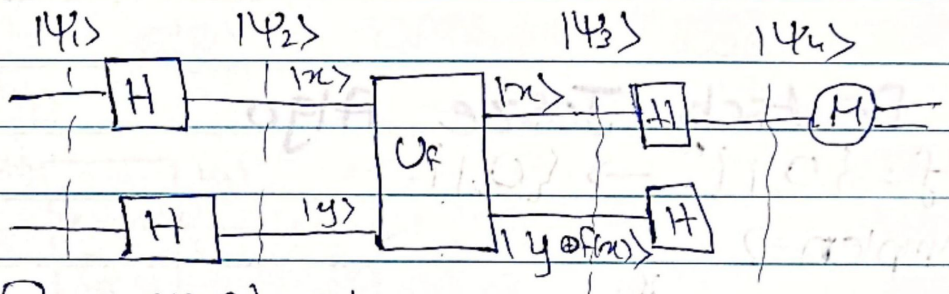
Deutsch Algo

Takes, gives one bit (0,1). Either it is constant or balanced. So, this algo finds if a func constant or balanced.

Constant		Constant		Balanced		Balanced	
x	f(x)	x	f(x)	x	f(x)	x	f(x)
0	0	0	1	0	0	0	1
1	0	1	1	1	1	1	0

case 1, case 2 — output always same; case 3, case 4 — output half

★ ⊕ is XOR in classical



if (M) = 0 constant

(M) = 1 balanced

Now lets test this algo on case 3.

$|\psi_1\rangle = |0\rangle|1\rangle = |01\rangle$ $\quad |\psi_2\rangle = |+\rangle|-\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

$$|\psi_2\rangle = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|\psi_3\rangle = U_f|\psi_2\rangle = \frac{1}{2}\left[|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle\right]$$

Foundation for Advancement of Science & Technology

$\therefore 0 \oplus f(x) = f(x)$
$1 \oplus f(x) = \overline{f(x)}$

$$|\psi_3\rangle = \frac{1}{2}\left[|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(0)\rangle - |1\rangle|\overline{f(1)}\rangle\right]$$

Now put values of $f(x), \overline{f(x)}$ acc. to case 3

$$|\psi_3\rangle = \frac{1}{2}\left(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle - |1\rangle|0\rangle\right)$$

$$= 1/2\left[|0\rangle(|0\rangle - |1\rangle) - |1\rangle(|0\rangle - |1\rangle)\right]$$

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

$|\psi_3\rangle = |-\rangle|-\rangle$

$|\psi_4\rangle = (H|-\rangle)(|-\rangle) = |1\rangle|-\rangle$

we measured and hence, func balanced.

Generalized: $|\psi_3\rangle = \pm|-\rangle|-\rangle$ (balanced)
$|\psi_3\rangle = \pm|+\rangle|-\rangle$ (constant)

Deutsch Josze Algo

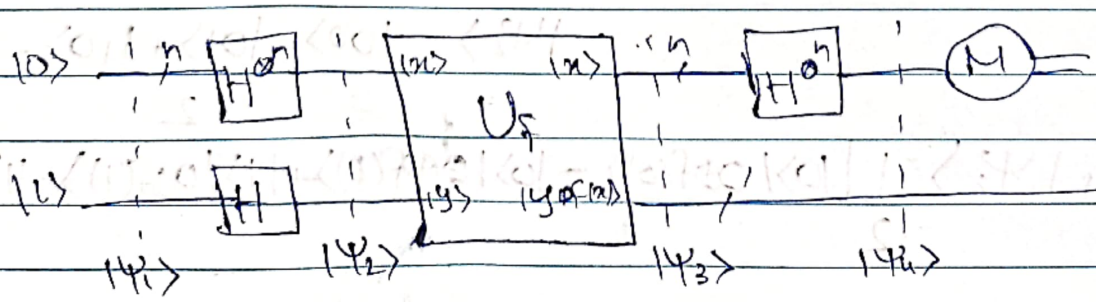
$f: \{0,1\}^n \rightarrow \{0,1\}$

For example $n=2$

x			x							
0	0	0	0	0	0	1	0	1	0	1
0	1	0	0	1	1	0	1	0	1	0
1	0	0	1	0	1	0	1	0	1	0
1	1	0	1	1	0	1	0	1	0	1

2 cases of constant

cases of balanced (half output)



Foundation for Advancement of Science & Technology

If you want to check that func is constant or balanced, then check half+1 bits, if a half+1 same then constant, if even one change then balanced. There are 2^n combinations, we check $\frac{2^n}{2}+1$ or $2^{n-1}+1$ so, $O(2^{n-1}+1) \approx O(2^n)$ ← exponential time

$2^n \cdot 2^{-1} \cdot 2^n$
2^{n-1}

General Case:

$|\psi_1\rangle = |0^n\rangle|1\rangle \quad |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|-\rangle$

$|\psi_3\rangle = U_f|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}$

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

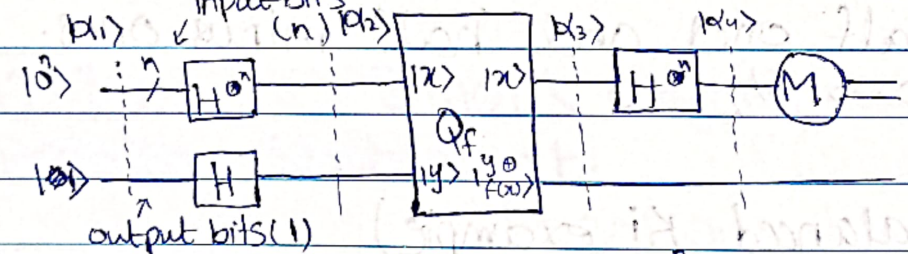
$\therefore f(x)=0 \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$

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

Let take case that constant with $f(x)=0$

7-3-24 $O(2^{n-1}+1)$ is time of classical and of quantum algo is $O(1)$. Now, we have to make such algo. L-12

Our claim: $|0^n\rangle \Rightarrow$ constant otherwise balanced



$|\alpha_1\rangle = |0^n\rangle|1\rangle \quad |\alpha_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|-\rangle \quad |\alpha_3\rangle = Q_f|\alpha_2\rangle$

$|\alpha_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \frac{|0\oplus f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}}$

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

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

Foundation for Advancement of Science & Technology

Hadamard Gate is linear gate, so it moves inside the summations. So, in $|\alpha_4\rangle$ we directly apply it on $|x\rangle$.

$$|\alpha_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \underbrace{(-1)^{f(x)}|-\rangle}_{\text{IT}} \quad \text{after Phase kickoff back}$$

$$|\alpha_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle |-\rangle \quad \text{we don't use it so we ignore it in next calculations.}$$

$$|\alpha_4\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \right]$$

now simplify both summations.

$$|\alpha_4\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)+x \cdot y} |y\rangle$$

We can check your claim now $\Rightarrow |y\rangle = |0^n\rangle$ with prob=1 if constant in this case all $x \cdot y = 0$ as $y=0$.

$(-1)^{f(x)}$ →
- $f(x)=0$ always: $(-1)^0 \Rightarrow \frac{1+1+1+1+\cdots(2^n\ 1\text{'s})}{2^n} = 1$
- $f(x)=1$ always: $(-1)^1 \Rightarrow \frac{-1-1-1-1-\cdots(2^n\ -1\text{'s})}{2^n} = -1$

in case of balanced, half ones and half minus ones. They cancel to make $0 \Rightarrow 0/2^n = 0$

Example $\Rightarrow$ n=2 (balanced Ki example)

x		f(x)					
0	0	1	1	1	0	0	0
0	1	1	0	0	1	1	0
1	0	0	1	0	1	0	1
1	1	0	0	1	0	1	1
					1		

decimal ↑

① ⇒

$|\alpha_1\rangle = |0^2\rangle|1\rangle = |001\rangle$

$|\alpha_2\rangle = \frac{1}{2}(|100\rangle + |101\rangle + |110\rangle + |111\rangle)$

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

$= \frac{1}{2}[|0\rangle + |1\rangle + |2\rangle + |3\rangle]|-\rangle$

Foundation for Advancement of Science & Technology

If changes sign where func returns 1.

$|\alpha_3\rangle = \frac{1}{2}[|0\rangle - |1\rangle - |2\rangle + |3\rangle]|-\rangle$ ← ignore it

$|\alpha_4\rangle = \frac{1}{2}\frac{1}{\sqrt{2^2}}|111\rangle(4) = |111\rangle$

	00	01	10	11
00(0)	+	+	+	+
-01(1)	-	+	-	+
-10(2)	-	-	+	+
11 (3)	+	-	-	+
	0	0	0	+4

Now, we take example of constant (all ones)
$|\alpha_2\rangle$ remains same, $|\alpha_3\rangle = 1/2[-|0\rangle - |1\rangle - |2\rangle - |3\rangle]$
$|\alpha_4\rangle = \frac{1}{2}\frac{1}{\sqrt{2^2}}[-(4)|00\rangle] = -|00\rangle$ Now when we measure, it comes

12-3-24 Simon's Algorithm L-13

Problem Statement: $f\{0,1\}^n \rightarrow \{0,1\}^n$

it is a 2 to 1 function, it means two inputs same output. Also, $f(x) = f(x \oplus s)$; s is a secret message, and our goal is to find s.

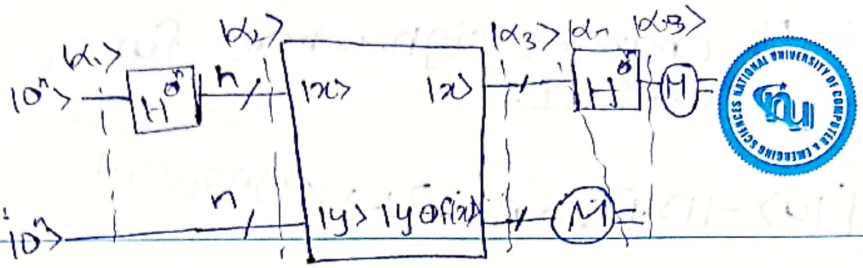
Example:- Let say $n=3$. lets $= 101$

input	output
000	110
001	011
010	000
011	111
100	011
101	110
110	111
111	000

so, if output at 000 is 110, then $000 \oplus 101$ is 101 so output at 101 shall also be 110.

Foundation for Advancement of Science & Technology

Quantum Circuit:



x	f(x)
0000, 1001	1111
0001, 1000	0001
0010, 1011	1110
0011, 1010	1101
0100, 1101	0000
0101, 1100	0101
0110, 1111	1010
0111, 1110	1001

To find s in classical, we would xor the two x values, it would take $O(2^n)$ time precisely $O(2^{n-1}+1)$. In Quantum, it would take $O(n)$ time.

$|\alpha_1\rangle = |10000\rangle |10000\rangle$ $\quad |\alpha_2\rangle = H^{\otimes 4} |0000\rangle |0000\rangle$

$= \frac{1}{\sqrt{2^4}} \sum_{x=0}^{15} |x\rangle |0000\rangle$

$|\alpha_3\rangle = \frac{1}{4} \sum_{x=0}^{15} |x\rangle |0000 \oplus f(x)\rangle = \frac{1}{4} \sum_{x=0}^{15} |x\rangle |f(x)\rangle$ ∴ XOR with 0 remain same.

$|\alpha_3\rangle = \frac{1}{4} [|0\rangle |f(0)\rangle + |1\rangle |f(1)\rangle + \cdots + |15\rangle |f(15)\rangle]$

in $|\alpha_4\rangle$ let say we measure f(8) ie f(9)

So, $|\alpha_4\rangle = [$]

$= \left[\frac{|0001\rangle + |1000\rangle}{\sqrt{2}}\right] |0001\rangle$ ∴ looking from table above.

Now for $|\alpha_5\rangle$ we have to apply $H^{\otimes n}$. So, we do that by taking some other $|\alpha_4\rangle$.

Let $|\alpha_4\rangle = \left(\frac{|0110\rangle + |1111\rangle}{\sqrt{2}}\right) |1010\rangle$

Foundation for Advancement of Science & Technology

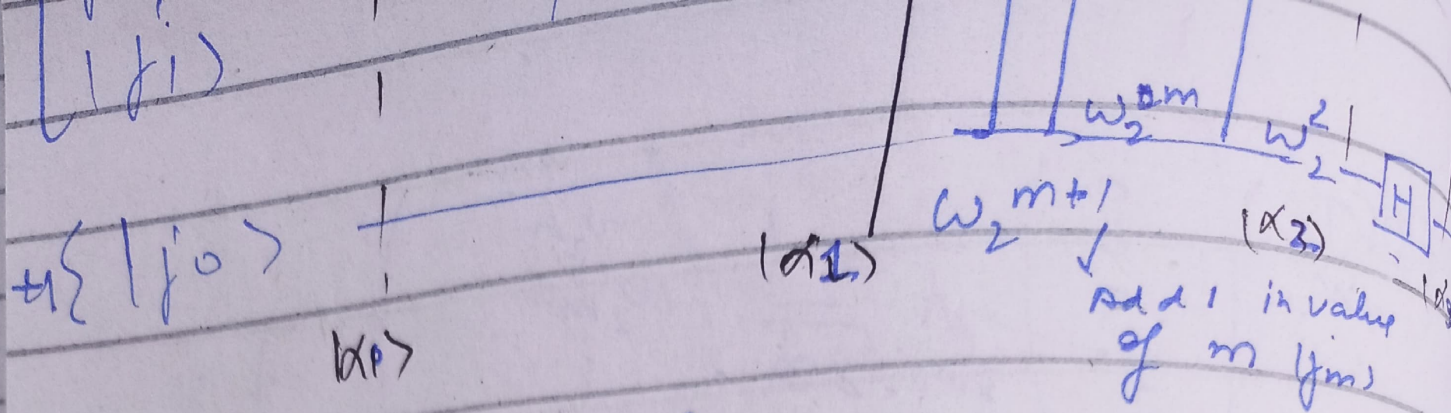
$$|\alpha_5\rangle = \frac{1}{\sqrt{2^3}}\left[|0000\rangle - |0010\rangle - |0100\rangle + |0110\rangle + |1001\rangle - |1011\rangle - |1101\rangle + |1111\rangle\right]$$

Now here all have equal probability, so we can measure any vector lets say 1101, then we save it and measure again. Continue it till n times, till we get n-1 linearly independant vectors.

Let say we get 1101, 1111, 1001. We ~~measure~~ calc s using:

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

S_1, S_2, S_3, S_4 are 4 bits of s.



→ we have circuit for 2^m qubits we are extending to 2^{m+1}

$$|\alpha_1\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} W_{2^m}^{jk} |k_0 k_1 \ldots k_{m-1}\rangle |j_0\rangle$$

→ bar

$$|\alpha_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{k=0}^{2^m-1} W_{2^m}^{jk}$$

After MID 2.

RSA (assymetric Algorithm)

(public, private key algo)

sender (Alice)	Hacker Oscar	Receiver (Bob)
		key generation
←		

Encryption	Decryption

Key generation:

1. p, q → prime no's (very large) 1024 bits for one prime no. for example we take small 3 & 11.
   - p = 3, q = 11
   - n → composite no. created by p & q $p \times q = 33$
2. $\phi(n)$ → totient fun, Euler phi fun.

$n = 3^5 \times 7^2 \times 11$.

Totient for number n

$\phi(n) = (3^5 - 3^4) \times (7^2 - 7^1) \times (11^1 - 11^0)$.

$= (3^1 - 3^0) \times (11^1 - 11^0) = 2 \times 10 = 20$

For 3×11 =

3. Public key e — such key whose multiplicate inverse exists. which exists when → $gcd(e, \phi(n)) = 1$

e = 3 here

4. Private key d: such $d \times e \equiv 1 \bmod \phi(n)$

d such that $e \times d \bmod \Phi(n) \equiv 1$.

$3 \times 2 = 6 \bmod 20 \neq 1$

$3 \times 7 = 21 \bmod 20 = 1$

public key → space of data

$(e, n) = (3, 33)$ → sent to sender.

Encryption:

Plaintext = x → what sender wants to send $= 2$.

$y = 2^{3} \bmod 33$ (3 → d, 33 → n)

$= 8$

Sender sends $y = 8$ to receiver.

Now, oscar knows $e = 3, n = 33, y = 8$

Decryption:

$x = y^{d} \bmod n = 8^{7} \bmod 33$

$= 2.$

$\Phi(100)$ ~~100~~ $100 = 2^2 \times 5^2$

5	100
5	20
2	4
	2

$= (2^2 - 2^1) \times (5^2 - 5^1)$

$= 2 \times 20 = 40$

(Shortcut method)

$8^2 \bmod 33 = 64 \bmod 33 = 31$

$8^3 \bmod 33 = 8 \times 31 \bmod 33$

$= 248 \bmod 33 = 17$

$8^4 \bmod 33 = 17 \times 8 \bmod 33.$

For Hacking :- → prime factors of n.

Oscar needs the value of p, q.

if he does he can find what user sent.

First he will find p, q.

$\phi(n) = (3-1) \times (11-1) = 20$

$3 \cdot d \equiv 1 \bmod 20$

→ to find inverse & gcd

Use extended euclidean algo to find d,

then $x = y^d \bmod n$ to find x.

One way problem here :-

↳ integer factorization.

SHOR can break it Algo

→ Since prime nos used are very large, its has very high time complexity

Euclidean Algo to find GCD in polynomial time :- (large no here, small here)

find gcd (64, 24) = gcd (24, 64 mod 24)

= gcd (16, 24 mod 16) = gcd (8, 16 mod 8)

gcd (8, 0) ; when we are done.

↓ 8 is gcd

Find gcd (20, 7) = gcd (7, 20 mod 7)

gcd = (6, 7 mod 6) = gcd (1, 6 mod 1)

gcd (1, 0) = 1.

↓ gcd = 1

→ when gcd 1 it means inverse of 7 exists in 20

SHOR Algo

CLASSICAL ALGO

gcd (33, 3) = 3 > 1 (factor)

gcd (33, 7) = 1 (not factor)

while (true) {

1- chose x ∈ {2, N-1}

2- if (d = gcd (N, x) > 1) { (it means we have got one prime factor of N.)

p = d, q = N/p

return (p, q) }

N too large, so can't technically find such d

quantum computer for this step.

$(x^{r/2})^2 \equiv 1 \bmod N$.

$(x^{r/2})^2 - (1)^2 = 0 \bmod N$.

$x^{r/2} - 1)(x^{r/2}+1) = 0 \bmod N$.

$p \times q$; $q \times \beta$.

order finding algo of quantum

③ find (order) r such that $x^r \equiv 1 \bmod N$.

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

④ if (r is even && $d == \gcd(x^{r/2}-1, N) > 1$)

{ $p = d$, $q = \frac{N}{p}$.

return (p, q) }.

if $x^{r/2} = \pm 1$ ↓ then trivial.

example $N = 221$

1- $x \in (2, 220)$. = $x = 5$

2- $\gcd(5, 221) = 1$

3- $x^r \equiv 1 \bmod 221$

$r = 8$

$5^1 \bmod 221 \neq 1$

5^2

4- $\gcd(5^4 - 1, 221) = \gcd(221, 624 \bmod 221)$

$= \gcd(182, 221 \bmod 182)$

$= \gcd(39, 182 \bmod 39) = \gcd(26, 39 \bmod 26)$

$= \gcd(13, 26 \bmod 13) = \gcd(13, 0) = 13$

p ↓ q

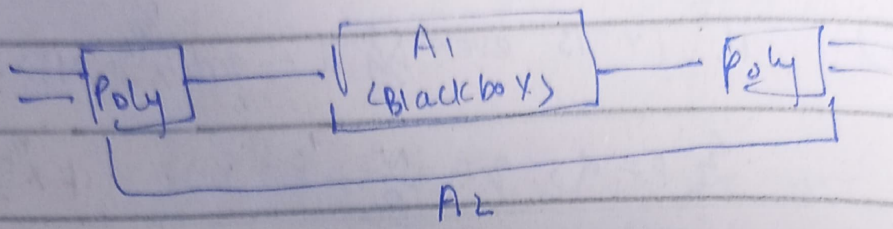
$p = 13$, $q = \frac{221}{13} = 17$.

return (13, 17)

N → [SHOR] → p, q

Shor $\leq_p$ order finding $\leq_p$ Phase estimation

polynomial time reducible



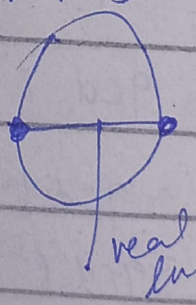
$A_2 \leq_p A_1$

Phase estimation Algo

Given a unitary matrix with dimension $U_{n \times n}$ and eigen vector of that matrix, $|u\rangle$, Estimate m-bit of θ such that

$U|u\rangle = e^{2\pi i\theta}|u\rangle$

values of hermitian matrix are on real line and of unitary it is on circle. If a matrix is both values lies on intersection of both



If we multiply eigen values of matrix we get its determinant.

So, if even one eigen value comes to be 0, then determinant is 0.

We also take area based on eigen values, So area also 0 if one eigen value is zero

we have a matrix $\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$

we find eigen values vectors.

we solve a characteristic eq. to find eigen value $|A - \lambda I| = 0$

For eigen vectors $(A - \lambda I)\vec{U} = 0$.

$$\begin{vmatrix} 1-\lambda & 2 \\ 3 & -1-\lambda \end{vmatrix} = 0$$

$$= (1-\lambda)(-1)(1+\lambda) - 3*2$$

$$= -1 + \lambda^2 - 6 = 0$$

$$\lambda^2 = 7, \Rightarrow \pm\sqrt{7} \rightarrow \text{non singular.}$$

Now vectors.

$$(A - \lambda I)\vec{U} = 0$$

For $\lambda = \sqrt{7}$ $\begin{pmatrix} 1-\sqrt{7} & 2 \\ 3 & -1-\sqrt{7} \end{pmatrix} \begin{pmatrix} U_1 \\ U_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

Applying gauss elimination $R_2 - \frac{3}{\sqrt{7}} R_1$

$$\begin{pmatrix} 1-\sqrt{7} & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

x_2 is free variable, For its any value we shall get x_1 value

Let $x_2 = 1$, so, $(1-\sqrt{7})x_1 + 2x_2 = 0$

$x_1 = \frac{-2}{1-\sqrt{7}}$ → we don't want sqrt in fraction.

So, $x_1 = \frac{-2}{1-\sqrt{7}} \times \frac{1+\sqrt{7}}{1+\sqrt{7}} = \frac{-2(1+\sqrt{7})}{-6}$

$= \frac{+1+\sqrt{7}}{3}$

So, $u \begin{pmatrix} \frac{1+\sqrt{7}}{3} \\ 1 \end{pmatrix}$ is correct ANS.

we write it as

$u = \begin{pmatrix} \frac{1+\sqrt{7}}{3} \\ 3 \end{pmatrix}$

Find eigen values of matrix

$$\begin{bmatrix} 3 & 0 \\ 2 & 4 \end{bmatrix}$$

$$|A - \lambda I| = 0$$

Step 1

$$\begin{bmatrix} 3 & 0 \\ 2 & 4 \end{bmatrix} - \lambda \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{vmatrix} 3-\lambda & 0 \\ 2 & 4-\lambda \end{vmatrix}$$

$$= (3-\lambda)(4-\lambda) =$$

$$= \boxed{\lambda_1 = 3}, \boxed{\lambda_2 = 4}.$$

Step 2: Find eigen vector corresponding to $\lambda_1 = 3$

Find x against each λ.

$$(A - \lambda I)\vec{x} = 0$$

$$(A - 3I)\vec{x} = 0$$

$$\begin{pmatrix} 3-3 & 0 \\ 2 & 4-3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \vec{0} \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \vec{0} \end{pmatrix}$$

$$\left(\begin{array}{cc|c} 0 & 0 & 0 \\ 2 & 1 & 0 \end{array}\right)$$

$$R_1 \leftrightarrow R_2$$

$$\left(\begin{array}{cc|c} 2 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

$x_2 = s$,

$2x_1 + x_2 = 0$

$2x_1 = -s$

$\boxed{x_1 = -s/2}$

To avoid fraction ANS, we can use x_2 as 2.

$\boxed{x_1 = -1}$, $\boxed{x_2 = 2}$.

eigen vector $\begin{pmatrix} -1 \\ 2 \end{pmatrix} = \vec{x_1}$ for $\lambda_1 = 3$

Find eigen vector for $\lambda_2 = 4$.

$(A - 4I)\vec{x} = 0$

$$\left(\begin{array}{cc|c} 3-4 & 0 & \\ 2 & 4-4 & \end{array}\right) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \bar{0}$$

$$\left(\begin{array}{cc|c} -1 & 0 & 0 \\ 2 & 0 & 0 \end{array}\right)$$

$R_2 = R_2 + 2R_1$

$$\left(\begin{array}{cc|c} -1 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

$x_2 = s = 1$

$x_1 = 0$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \vec{X_2}$$

verify: $A\vec{x} = \lambda\vec{x}$

$$\begin{bmatrix} 3 & 0 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} -1 \\ 2 \end{bmatrix} = 3 \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

$$\begin{bmatrix} -3 \\ 6 \end{bmatrix} = 3 \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

$$3 \begin{bmatrix} -1 \\ 2 \end{bmatrix} = 3 \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

verified.

$$\begin{bmatrix} 3 & 0 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 4 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 4 \end{bmatrix} = 4 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$4 \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 4 \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Eigen vector / value rules.

① eigen vector cannot be 0.

② two eigen vector can have same eigen values

$$x_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \lambda_1 = 2 \qquad \begin{bmatrix} 2 & * \\ 0 & 2 \end{bmatrix}$$

$$x_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \lambda_2 = 2$$

③ $A_{N \times N}$ can have at most n linearly independent vectors

④ If $A\vec{x} = \lambda\vec{x}$ then $A\vec{y} = \lambda\vec{y}$

where $\vec{y} = a\vec{x}$

⑤ Trace Rule:

Sum of eigen values = trace.

$$\begin{bmatrix} 1 & 2 & \\ 2 & 2 & 0 \\ 4 & 1 & 3 \end{bmatrix} \quad 1+2+3 = 6 \rightarrow \text{trace.}$$

⑥ $|A| = \lambda_1 \times \lambda_2 \times \ldots \lambda_n$

⑦ Diagonal rule:

$$\begin{bmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix}.$$

$\lambda_1 = a_{11}$, $\lambda_2 = a_{22}$, $\lambda_3 = a_{33}$

If matrix was like this

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

$\vec{x_1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, $\vec{x_2} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$, $\vec{x_3} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$.

If matrix was like this $\lambda_1 = a_{11}$, $\lambda_2 = a_{22}$, $\lambda_3 = a_{33}$

$$\begin{bmatrix} a_{11} & 0 & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{bmatrix}$$ → partially diagonal

$$\bar{x}_1 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad x_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

(8) TRIANGULAR MATRIX

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix}.$$

$\lambda_1 = a_{11}$, $\lambda_2 = a_{22}$, $\lambda_3 = a_{33}$.

$x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$, x_2 & x_3 → find by long method

(9) eigen values of A = eigen values of A^T.

(10) If λ is eigen value of A than λ^k is eigen value of A^k.

A: $\lambda_1 = 5$, $\lambda_2 = 2$.

A^2: $\lambda_1 = 25$, $\lambda_2 = 6$.

A^{-1}: $\lambda_1 = \frac{1}{5}$, $\lambda_2 = \frac{1}{3}$.

(11) If any eigen value is 0.
$|A|$ is 0, singular, no linear indep. vectors

(12) All rows of matrix has same sum S. then one eigen value will be $\lambda_i = S$. and its corresponding vector will contain all 1's

$$x = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$$

Phase estimation Algo

Ex Given a unitary matrix

$U = -i|0\rangle\langle 0| + i|1\rangle\langle 1|$ and eigen vector

$|V\rangle = |0\rangle$, estimate 2-bit of $\theta \in [0,1)$

such that $U|V\rangle = e^{2\pi i\theta}|V\rangle$

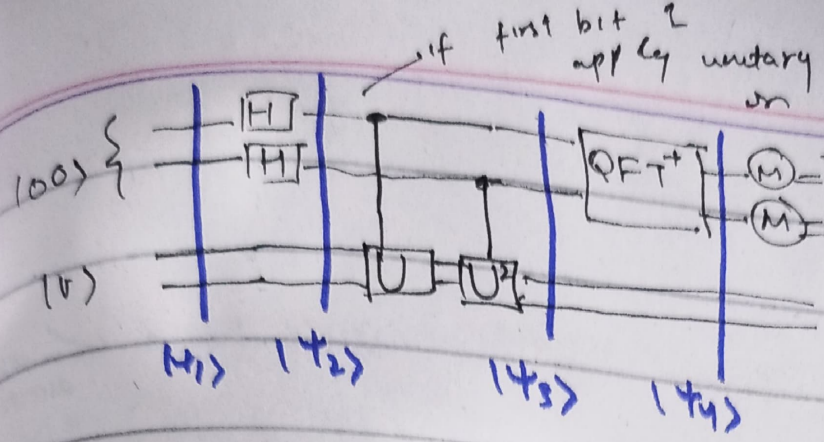
$\therefore$ eigen value

$$U = \begin{pmatrix} -i & 0 \\ 0 & +i \end{pmatrix}$$

Size of first register = 2 bits = n

" " second depends on unitary matrix

so also 2 bits = n takes eigen vector as input



result of measurement is value y.

$\theta = y/m.$

$2 \rightarrow 2.$

$\theta = y/4.$

$|\psi_1\rangle = |00\rangle|v\rangle$

$|\psi_2\rangle = H^{\otimes 2}|00\rangle|v\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{2^2}} \sum_{0}^{3} |x\rangle|v\rangle$

$|\psi_2\rangle = \frac{1}{2}\left[|0\rangle + |1\rangle + |2\rangle + |3\rangle\right]|v\rangle.$

$|\psi_3\rangle = \frac{1}{2}\sum_{x=0}^{3} |x\rangle U^{x}|v\rangle.$

U^x replaced by eigen value.

$= \frac{1}{2}\sum_{x=0}^{3} |x\rangle(-i)^x|v\rangle$

Phase kickback.

$|\psi_3\rangle = \frac{1}{2}\sum_{0}^{3} (-i)^x |x\rangle|v\rangle$

Since we measure first register from now on, so, don't write it

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

$= \frac{1}{2}\left[|0\rangle - i|1\rangle + |2\rangle + i|3\rangle\right]$

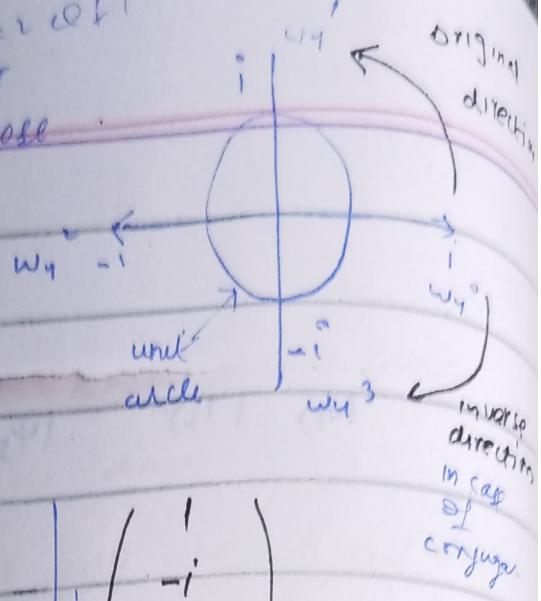
$|\psi_4\rangle = QFT^{+}|\psi_3\rangle$

$QFT_4 = \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & w_4 & w_4^2 & w_4^3 \\ 1 & w_4^2 & w_4^4 & w_4^6 \\ 1 & w_4^3 & w_4^6 & w_4^9 \end{pmatrix}$

Take conjugate transpose

$w_4 = e^{2\pi i/4}$

$w_4 = e^{\pi/2 i}$



$$QFT_4^{+} = \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 \\ -i \\ -1 \\ i \end{pmatrix}$$

Multiply $|\psi_3\rangle$ with this to get $|\psi_4\rangle$

$$= \frac{1}{4} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 4 \end{pmatrix} = |3\rangle.$$

After measuring y will be 3.

$$\theta = y/4 = 3/4$$

$$\lambda = e^{2\pi i 3/4} = -i$$

correct value of eigen