Foundation for Advancement of Science & Technology

Dirac's Bra Ket Notation & Tensor Product (Video lecture)

1) Ket-Notation $|-\rangle$

2) Bra-Notation $\langle-|$

3) Ket-Ket $|-\rangle|-\rangle$

5) KetBra $|-\times-|$ → 4) Bra-Bra $\langle-|\langle-|$

6) Braket $\langle-|-\rangle$

1) Ket-Notation:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{matrix} \leftarrow 0^{th} \text{ location} \\ \leftarrow 1^{st} \text{ "} \end{matrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

e.g.

$|101\rangle =$

$2^3 = 8$

8 dimensional vector

$$\begin{pmatrix} 0 \leftarrow 0^{th} \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \leftarrow 5^{th} \\ 0 \\ 0 \leftarrow 7^{th} \end{pmatrix}$$

- 101 in decimal is 5, therefore we place 1 in the 5^{th} position in the 8 dimensional vector

$|11\rangle =$

$2^2 = 4D$

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

→ We can represent any column vector in any dimension in the power of 2

- 2D.

$\{|0\rangle, |1\rangle\}$ (Standard Basis)

$$\begin{pmatrix} 7 \\ 3+5i \end{pmatrix} = 7|0\rangle + (3+5i)|1\rangle$$

- 4D

$$\begin{pmatrix} 7 \\ 0 \\ i+3 \\ 0 \end{pmatrix} = 7|00\rangle + (i+3)|10\rangle, |11\rangle$$

Basis: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

2) Bra-Notation:

$\langle 0| = [1 \; 0]$, $\langle 1| = [0 \; 1]$

$|\psi\rangle^{\dagger} = \langle\psi|$, $\langle\psi|^{\dagger} = |\psi\rangle$

$\dagger$ = conjugate transpose

(conjugate: change sign of every term having iota)

(transpose: convert rows to columns & columns to rows)

e.g

$|\psi\rangle = (3+5i)|0\rangle + 7|1\rangle$

Find what is $\langle\psi|$.

$\Rightarrow \langle\psi| = |\psi\rangle^{\dagger} = (3-5i)\langle 0| + 7\langle 1|$

$|\psi\rangle = \begin{pmatrix} 3+5i \\ 7 \end{pmatrix}$, $\langle\psi| = [3-5i \quad 7]$

→ Representing vector in Bra-notation:

$[3 \; 0 \; i \; 7] = 3\langle 00| + i\langle 10| + 7\langle 11|$

3) Ket-Ket notation:

Gives us the tensor product of column vectors creating a column vector of higher dimensions. Similarly, BraBra notation gives us the tensor product of 2 row vectors.

* Generally knowing tensor product is important, as it will be later used to create Quantum Gates.

⇒ Tensor Product: ⊗

$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 7 \end{pmatrix}$

$$A \otimes B = \begin{pmatrix} 1.B & 0.B \\ 0.B & 2.B \end{pmatrix}$$

$$= \begin{pmatrix} 1\,2\,3 & 0\,0\,0 \\ 0\,4\,7 & 0\,0\,0 \\ 0\,0\,0 & 2\,4\,6 \\ 0\,0\,0 & 0\,8\,14 \end{pmatrix}$$ Higher Dimensional Matrix

⇒ ket-ket:

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle|\phi\rangle = |\psi\phi\rangle$$ [All represent tensor product]

e.g

$$|\psi\rangle = i|0\rangle + 7|1\rangle \;,\; |\phi\rangle = |00\rangle + 3|10\rangle + 7|11\rangle$$

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

Representing in vectors:

$$|\psi\rangle = \begin{pmatrix} i \\ 7 \end{pmatrix} \;,\; \phi = \begin{pmatrix} 1 \\ 0 \\ 3 \\ 7 \end{pmatrix}$$

$$|\psi\phi\rangle = \begin{pmatrix} i & — & 0 \\ 0 & — & 1 \\ 3i & — & 2 \\ 7i & — & 3 \\ 7 & — & 4 \\ 0 & — & 5 \\ 21 & — & 6 \\ 49 & — & 7 \end{pmatrix}$$

Foundation for Advancement of Science & Technology

4) Bra-Bra notation:

e.g

$\langle\psi| = 3\langle 0| + 7\langle 1|$, $\langle\phi| = \langle 0| + i\langle 1|$

$\langle\psi| \otimes \langle\phi| = \langle\psi\phi| = 3\langle 00| + 3i\langle 01| + 7\langle 10| + 7i\langle 11|$

Representing as vectors :

$\langle\psi| = [3 \quad 7]$ $\langle\phi| = [1 \quad i]$

$\langle\psi\phi| = [3 \quad 3i \quad 7 \quad 7i]$

5) Ket-Bra notation:

$|\alpha\rangle\langle\beta| = |\alpha X \beta|$.

Result of this operation will always be a matrix and no matter the dimension of the vectors the operation will be valid.

$|\alpha \quad X \quad \beta|$

$m \times 1 \quad 1 \times n$

$= m \times n$

e.g

$|00\rangle\langle 10| = |00 \; X \; 10|$ (row, col)

$= \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} [0 \; 0 \; 1 \; 0] = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

e.g

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

$|\alpha \times \beta| = ?$

$\rightarrow \langle\beta| = |\beta\rangle^{\dagger} = \langle 00| + 2\langle 10| + 7\langle 11|$

$|\alpha \times \beta| = (3|0\rangle + i|1\rangle)(\langle 00| + 2\langle 10| + 7\langle 11|)$

$= 3|0\times 00| + 6|0\times 10| + \cancel{2i|0\times 00|} + 21|0\times 11| + i|0\times 00| + 2i|1\times 10| + 7i|1\times 11|$

Representing as matrix:

matrix has 2^1 rows & 2^2 columns : (2x4)

$$\begin{bmatrix} 3 & 0 & 6 & 21 \\ i & 0 & 2i & 7i \end{bmatrix}$$

0th row, 1st row

0th col, 1st, 2nd, 3rd

e.g.

$$A = \begin{pmatrix} 0 & 1 \\ 3 & i \\ 7 & 0 \\ 0 & 13 \end{pmatrix}$$

0 (00) 1 (01) 2 (10) 3 (11)

Express using Ket-Bra

$= |00\times 1| + 3|01\times 0| + i|01\times 1| + 7|10\times 0| + 13|11\times 1|$

Foundation for Advancement of Science & Technology

6) Bra-Ket Notation:

$\langle \alpha | \beta \rangle$

$1 \times n$ $\quad$ $m \times 1$ $\quad$ $1 \times 1 = \text{number}$.

$n = m$.

- The result of this multiplication is a number. This number is called the inner product of this number.

e.g. $\langle 1|1\rangle = 1$

$$\langle 0|0\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1 \times 1 + 0 \times 0 = 1$$

- If inner product of a vector with itself is equal to 1 then it implies that its magnitude will also be equal to 1

Norm:

$|\alpha\rangle$ is $\sqrt{\langle \alpha | \alpha \rangle}$. If $\sqrt{\langle \alpha|\alpha\rangle} = 1$ then it is called unit vector

Orthogonal:

when $\langle \alpha | \beta \rangle = 0$.

$$\langle 0|1\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1(0) + 0(1) = 0.$$

Foundation for Advancement of Science & Technology

e.g.

$|\alpha\rangle = i|0\rangle + 7|1\rangle$, $|\beta\rangle = 3|0\rangle + i|1\rangle$. Calculate inner product.

→ $\langle\alpha|\beta\rangle = ?$

$\langle\alpha| = |\alpha\rangle^{\dagger} = -i\langle 0| + 7\langle 1|$

$\langle\alpha|\beta\rangle = (-i\langle 0| + 7\langle 1|)(3|0\rangle + |1\rangle)$

$= -3i\underbrace{\langle 0|0\rangle}_{=1} - i\underbrace{\langle 0|1\rangle}_{=0} + 21\underbrace{\langle 1|0\rangle}_{=0} + 7\underbrace{\langle 1|1\rangle}_{=1}$

$= -3i + 7$ (inner product)

- Remember inner product is not commutative.

For real number, $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle$

" complex ", $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^{*}$ (conjugate)

Foundation for Advancement of Science & Technology

Quantum Computing
Qubits & Measurements (Video Lec #2)

Classical Computers: unit of data: bit (0 or 1)

Quantum computers: unit of data: qubit

States of qubit:

① pure state (classical state): 0 or 1

② & Superposition state (quantum state): 0 and 1
with prob p, with prop 1-p

Math Representation:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α & β are amplitudes of qubits.

- α & β are compler numbers and can also take -ve values

Prob of 0 = $|\alpha|^2$ where $|\alpha|^2 = \alpha^* \alpha$

Prob of 1 = $|\beta|^2$ where $|\beta|^2 = \beta^* \beta$

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

- $|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ (unit vector)

$\| |\psi\rangle \| = 1$ or $\langle \psi | \psi \rangle = 1$

Foundation for Advancement of Science & Technology

Example:

Q) $|\psi\rangle = \frac{-4i}{5}|0\rangle + \frac{3}{5}|1\rangle$

a) Is $|\psi\rangle$ a valid qubit

b) What is the probability we get 1.

a) we can either compute $|\alpha|^2 + |\beta|^2 = 1$ or $\| |\psi\rangle \| = 1$ or $\langle\psi|\psi\rangle = 1$.

$\alpha = \frac{-4i}{5}$, $\beta = \frac{3}{5}$

$|\alpha|^2 = \alpha^* \alpha = \frac{4i}{5} \times \frac{-4i}{5} = \frac{16}{25}$, $|\beta|^2 = \beta^* \beta = \frac{3}{5} \times \frac{3}{5} = \frac{9}{25}$

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

$\frac{16}{25} + \frac{9}{25} = 1$

$1 = 1$ ✓ (valid Qubit).

b) Prob of $0 = \left|\frac{-4i}{5}\right|^2 = \frac{16}{25} = 0.64$

Prob of $1 = \left|\frac{3}{5}\right|^2 = \frac{9}{5} = 0.36$

or

Prob of 1 = $1 - 0.64 = 0.36$.

Foundation for Advancement of Science & Technology

Q. $|\psi\rangle = \frac{-4}{5}i\,|0\rangle + \frac{3}{5}|1\rangle$, $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$$|\psi\rangle \otimes |\phi\rangle = |\psi\phi\rangle = \left(\frac{-4}{5}i|0\rangle + \frac{3}{5}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \underset{\alpha}{\frac{-4}{5\sqrt{2}}}|00\rangle + \underset{\beta}{\frac{-4}{5\sqrt{2}}}|01\rangle + \underset{\gamma}{\frac{3}{5\sqrt{2}}}|10\rangle + \underset{\delta}{\frac{3}{5\sqrt{2}}}|11\rangle$$

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

- Probability of $00 = |\alpha|^2 = \alpha^*\alpha = \frac{-4}{5\sqrt{2}} \times \frac{-4}{5\sqrt{2}} = \frac{16}{50} = 0.32$

Operations on Qubits:

① Measure (Full or Partial)

② Transform using quantum gates

Foundation for Advancement of Science & Technology

Quantum Computing

Full & Partial Measurements of Qubits

(video lec # 3)

Rules:

① If the measured Qubits are in superposition, then after measurement they change into pure state

② The new resultant state should fulfil the normalization constraint

Example:

$|\psi\rangle = \frac{1}{2}|00\rangle - \frac{i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$ (Full Measurement)

Measurements	Prob	Resultant state
00	$\left\|\frac{1}{2}\right\|^2 = \frac{1}{4} = 0.25$	$\|\psi\rangle = \|00\rangle$ (pure state)
10	$\left\|\frac{-i}{2}\right\|^2 = \frac{i}{2} \times \frac{-i}{2} = 0.25$	$\|\psi\rangle = \|10\rangle$ "
11	$\left\|\frac{1}{\sqrt{2}}\right\|^2 = \frac{1}{2} = 0.5$	$\|\psi\rangle = \|11\rangle$ "

(Partial Measurement)

Measurements	Prob	Resultant state
1st qubit = 1	$\left\|\frac{-i}{2}\right\|^2 + \left\|\frac{1}{\sqrt{2}}\right\|^2 = \frac{3}{4}$	$\|\psi\rangle = \frac{\frac{-i}{2}\|10\rangle + \frac{1}{\sqrt{2}}\|11\rangle}{\left\\|\frac{-i}{2}\|10\rangle + \frac{1}{\sqrt{2}}\|11\rangle\right\\|}$

$$= \left(\frac{-i}{2}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) \Big/ \sqrt{\frac{3}{4}}$$

$$= \frac{-i}{\sqrt{3}}|10\rangle + \frac{\sqrt{2}}{\sqrt{3}}|11\rangle$$

Foundation for Advancement of Science & Technology

2nd Measurement	Probability	Resultant state
Qubit = 0	$\left\|\frac{1}{2}\right\|^2 + \left\|\frac{-i}{2}\right\|^2$	$\lvert\psi\rangle = \frac{\frac{1}{2}\lvert 00\rangle - \frac{i}{2}\lvert 10\rangle}{\sqrt{\frac{1}{2}}}$
	$= \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$	$= \frac{\sqrt{2}}{2}\lvert 00\rangle - \frac{\sqrt{2}}{2} i \lvert 10\rangle$

Example:

Q) $\frac{1}{\sqrt{5}}\lvert 0000\rangle - \sqrt{\frac{2}{5}}\lvert 0100\rangle + \sqrt{\frac{1}{5}}\lvert 1111\rangle + \sqrt{\frac{1}{5}}\lvert 0110\rangle$. What is the probability & resultant state if 1st & 4th qubits are = 0.

$\Rightarrow P(A \cup B \cup C) = P(A) + P(B) + P(C)$.

Probability = $\left|\frac{1}{\sqrt{5}}\right|^2 + \left|\sqrt{\frac{2}{5}}\right|^2 + \left|\sqrt{\frac{1}{5}}\right|^2 = \frac{1}{5} + \frac{2}{5} + \frac{1}{5} = \frac{4}{5}$

Resultant state = $\lvert\psi\rangle = \left(\frac{1}{\sqrt{5}}\lvert 0000\rangle - \sqrt{\frac{2}{5}}\lvert 0100\rangle + \sqrt{\frac{1}{5}}\lvert 0110\rangle\right) \Big/ \sqrt{\frac{4}{5}}$

$= \frac{1}{2}\lvert 0000\rangle - \frac{1}{\sqrt{2}}\lvert 0100\rangle + \frac{1}{2}\lvert 0110\rangle$

Foundation for Advancement of Science & Technology

Quantum Computing

Qubit Measurements in Various Orthonormal Bases

Video# Lecture #

- Standard Basis: a set of linearly independent vectors where each vector has exactly 1 in it where rest of the vectors in it are all 0's

2D: $\left\{\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right\}$ ✓

$= \{|0\rangle, |1\rangle\}$ ✓

3D: $\left\{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}\right\}$ ✓

4D: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

Orthonormal Basis: contains orthogonal vectors which are also normalized (unit vector).

1) Normalized "unit vector"
2) Orthogonal "ith"

Hadamard Basis: $\{|+\rangle, |-\rangle\}$

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

Foundation for Advancement of Science & Technology

- Check if it is unit vector

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

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

$$= \sqrt{\frac{1}{2}\left[\underbrace{\langle 0|0\rangle}_{=1} + \underbrace{\langle 0|1\rangle}_{=0} + \underbrace{\langle 1|0\rangle}_{=0} + \underbrace{\langle 1|1\rangle}_{=1}\right]}$$

$$= \sqrt{\frac{1}{2}[2]} = 1 \checkmark$$

$$\| |-\rangle \| = \sqrt{\langle -|-\rangle} = 1 \ ?$$

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

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

$$= \sqrt{\frac{1}{2}[2]} = 1 \checkmark$$

- Check if orthogonal (inner product equals zero)

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

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

$$= \frac{1}{2}[0] = 0 \checkmark$$

Foundation for Advancement of Science & Technology

Formula:

$\{ |\alpha\rangle, |\beta\rangle \}$

$$|\psi\rangle = \underbrace{\langle\psi|\alpha\rangle}_{\text{amplitude of } |\alpha\rangle} \cdot |\alpha\rangle + \underbrace{\langle\psi|\beta\rangle}_{\text{amplitude of } |\beta\rangle} \cdot |\beta\rangle$$

Probability of measuring $|\alpha\rangle = |\langle\psi|\alpha\rangle|^2$

Probability of measuring $|\beta\rangle = |\langle\psi|\beta|^2$

Example:

Q) $|\psi\rangle = |0\rangle$

(Standard Basis)

Prob of (M) $0 = |1|^2 = 1$

Prob of (M) $1 = 0$

(Hadamard Basis):

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

Prob of (M) $|+\rangle = |\langle\psi|+\rangle|^2 = \left|(\langle 0|)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\right|^2$

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

$$= \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} = \frac{1}{2}$$

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

Foundation for Advancement of Science & Technology

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

Sol) Hadamard Basis:

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

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

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

Standard Basis:

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

Prob of (M) $|0\rangle = |\langle\psi|0\rangle|^2 = \left|\left[\left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\langle+| + \left(\frac{1}{\sqrt{6}} + \frac{1}{\sqrt{3}}\right)\langle-|\right] \cdot |0\rangle\right|^2$

$= \left|\left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{3}}\right)\langle+|0\rangle + \left(\frac{1}{\sqrt{6}} + \frac{1}{\sqrt{3}}\right)\langle-|0\rangle\right|^2$

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

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

$= \left|\frac{1}{\sqrt{2}}\left(\frac{2}{\sqrt{6}}\right)\right|^2 = \left|\frac{1}{\sqrt{3}}\right|^2 = \boxed{\frac{1}{3}}$

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

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

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

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

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

Foundation for Advancement of Science & Technology

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

Foundation for Advancement of Science & Technology

Quantum Computing

Quantum Gates

Unitary matrix

$U|\alpha\rangle = |\beta\rangle$ (transform qubit(s))

qubit(s)

operation

- The ~~function~~ that preserves the norm of a vector is called unitary matrix

Unitary Matrix:

$$U^\dagger U = UU^\dagger = I$$

$$U^\dagger = U^{-1}$$

If these 2 properties are true then.

$$A^{-1} = A$$

Hermitian Matrix:

$$H^\dagger = H$$

Taking conjugate transpose of a matrix produces the same matrix

e.g

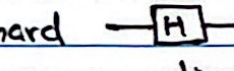
$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ Test if matrix is unitary & hermission

$Y^\dagger = \begin{pmatrix} 0 & -i \\ +i & 0 \end{pmatrix} \Rightarrow Y^T = Y$ Hermitian Matrix ✓

$Y^\dagger Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i*i & 0 \\ 0 & -i*i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Unitary Matrix ✓

Foundation for Advancement of Science & Technology

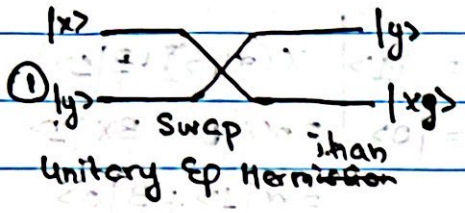
Quantum Gates: (Single Qubit)

GATE	Matrix	Examples
① Pauli-X  Unitary & Hermitian	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$X\|0\rangle = \|1\rangle$ $X\|1\rangle = \|0\rangle$ $X(\alpha\|0\rangle + \beta\|1\rangle)$ $= \alpha X\|0\rangle + \beta X\|1\rangle$ $= \alpha\|1\rangle + \beta\|0\rangle$
② Pauli-Z  Unitary & Hermitian	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$Z\|0\rangle = \|0\rangle$ $Z\|1\rangle = -\|1\rangle$ $Z(\alpha\|0\rangle + \beta\|1\rangle)$ $= \alpha\|0\rangle - \beta\|1\rangle$
③ Hadamard  Unitary & Hermitian	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	$H\|0\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}} = \|+\rangle$ $H\|1\rangle = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}} = \|-\rangle$ $H\|+\rangle = \|0\rangle$, $H\|-\rangle = \|1\rangle$
④ Rotation  Unitary but not Hermitian	$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$	$R_\theta \neq R_\theta^\dagger$ $R_\theta^\dagger R_\theta = 1$

Foundation for Advancement of Science & Technology

2 Qubits

GATE	Matrix	Examples

① 

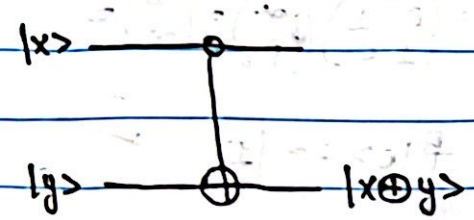
Unitary & Hermitian

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

SWAP $|01\rangle = |10\rangle$

② CNOT (Control Gate)

Control bit (if control bit 1 then second bit is flipped)



U & H

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

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

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

↑ if 0 it remains the same

To make control gate out of any single qubit gate: $^{(U)}$

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

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

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

Foundation for Advancement of Science & Technology

Quantam Computing
Understanding the Hadamard Gate

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Applying Hadamard gate,

$$H|\psi\rangle = |\psi'\rangle$$

- A key use of hadamard gate is that given an input qubit in pure state it creates a qubit in equal superposition state

eg

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{(we can get 0 \& 1 with same probability)}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad " \quad " \quad "$$

Verifying above result,

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1+0 \\ 1+0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]$$ ✓

Unitary:

$$HH^{+} = I$$

$$\Rightarrow H^{-1} = H$$

Hermitian:

$$H = H^{+}$$

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

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

$$= \frac{2|1\rangle}{2} = |1\rangle$$

Applying hadamard gate on equal superposition $H|1\rangle$ we get $|1\rangle$

Hadamard gate on multiple qubits:-

$H^{\otimes 2}|00\rangle$ (⊗ : tensor product)

Method 1: Matrices

$H^{\otimes 2}|00\rangle$

→ $H^{\otimes 2} = H \otimes H$

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

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

$$H^{\otimes 2}|00\rangle = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}\begin{pmatrix}1\\ 0\\ 0\\ 0\end{pmatrix}$$

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

Foundation for Advancement of Science & Technology

Method 2:

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

$$H^{\otimes 2}|00\rangle = H^{\otimes 2}[|0\rangle|0\rangle]$$
$$= H|0\rangle\, H|0\rangle$$
$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Hadamard Gate's General Expression:

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

n: no. of qubits

$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=1}^{n^2} |y\rangle$$ Simplified Version

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

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

$$H|x\rangle = \hat{} \sum_{y \in \{0,1\}}^{1/\sqrt{2}} (-1)^{xy} |y\rangle \quad - (1)$$

Single qubit registers

$$H^{\otimes 2}|x\rangle = H|x_1\rangle \otimes H|x_2\rangle$$
$$x \in \{0,1\}^n = \left(\frac{1}{\sqrt{2}} \sum_{y_1 \in \{0,1\}} (-1)^{x_1 y_1} |y_1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}} \sum_{y_2 \in \{0,1\}} (-1)^{x_2 y_2} |y_2\rangle\right)$$
$$= \frac{1}{\sqrt{2^2}} \sum_{y \in \{0,1\}^2} (-1)^{x_1 y_1 + x_2 y_2} \otimes |y\rangle$$

Foundation for Advancement of Science & Technology

Q. What is $H^{\otimes 3}|101\rangle$

$$H^{\otimes 3}|x\rangle = \frac{1}{\sqrt{2^3}} \cdot \sum_{y \in \{0,1\}^n} (-1)^{x.y} |y\rangle$$

$$H^{\otimes 3}|101\rangle = \frac{1}{\sqrt{2^3}} \Big[(-1)^{1.0+0.0+1.0} |000\rangle + (-1)^{1.0+0.0+1.1} |001\rangle + (-1)^{1.0+0.1+1.0} |010\rangle + (-1)^{1.0+0.1+1.1} |011\rangle + (-1)^{1.1+0.0+1.0} |100\rangle + (-1)^{1.1+0.0+1.1} |101\rangle + (-1)^{1.1+0.1+1.0} |110\rangle + (-1)^{1.1+0.1+1.1} |111\rangle \Big]$$

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

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

e.g. $H^{\otimes 3}\left(\frac{|000\rangle + |110\rangle - |100\rangle - |111\rangle}{\sqrt{4}}\right)$ (2^3 = 8 cols)

All signs +ve if min no. of 1's in sign are -ve	000	001	010	011	100	101	110	111
000	+	+	+	+	+	+	+	+
110	+	+	−	−	−	−	+	+
−100	✗ −	✗ −	✗ −	✗ −	✗ +	✗ +	✗ +	✗ +
−111	✗ −	✓ +	✓ +	✗ −	✓ +	✗ −	✗ −	✓ +

→ if first 2 locations have even no. of 1's sign will be +ve (+) & (−) otherwise ignore last location.

if first location has 1 then sign will be -ve. If zero sign would be +ve

Because of minus sign in −100 we flip all signs

$$= \frac{1}{\sqrt{4}} \cdot \frac{1}{\sqrt{2^3}} \left(2|001\rangle - 2|011\rangle + 2|100\rangle + 2|110\rangle + 4|111\rangle \right)$$

Foundation for Advancement of Science & Technology

Quantum Computing

Controlled NOT (CNOT) Quantum Gate

Unitary: $CNOT \times CNOT^{\dagger} = I$

$CNOT^{\dagger} = CNOT^{-1}$

Hermission: $CNOT = CNOT^{\dagger}$

$\Rightarrow CNOT^{-1} = CNOT$

$CNOT(CNOT|x\rangle) = |x\rangle$

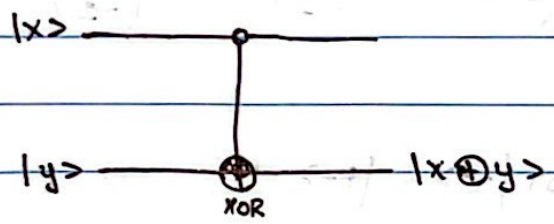
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$CNOT|00\rangle = |00\rangle$

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

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

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

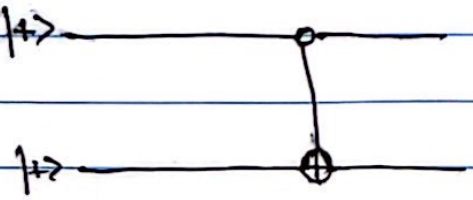


Verify $CNOT|11\rangle = |10\rangle$

$$CNOT|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle$$

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

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



$CNOT|++\rangle = |++\rangle$

$CNOT|-+\rangle = |-+\rangle$

$CNOT|--\rangle = |+-\rangle$

$CNOT|+-\rangle = |--\rangle$

if 2nd qubit = +, the no flip

if 2nd qubit = −, the flip 1st

Foundation for Advancement of Science & Technology

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

$$= \frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{\sqrt{2}\cdot\sqrt{2}} \qquad = \frac{1}{2}\,|00\rangle - |01\rangle + |10\rangle - |11\rangle$$

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

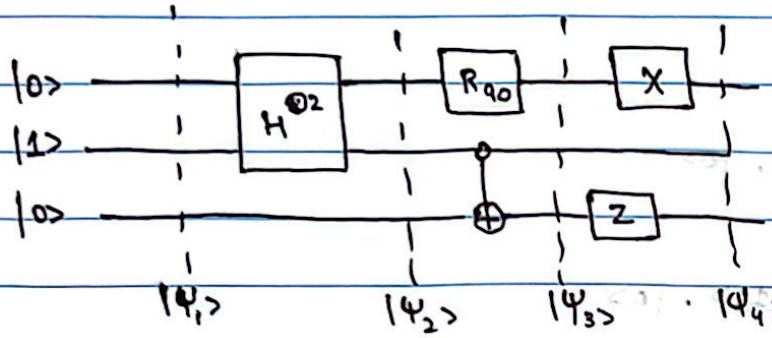
$$\text{CNOT}\,|--\rangle = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

Therefore, $\text{CNOT}\,|--\rangle = |+-\rangle$ ✓

Foundation for Advancement of Science & Technology

Quantum Computing

Quantum circuits



a) Make reverse circuit

b) Write output of the circuit

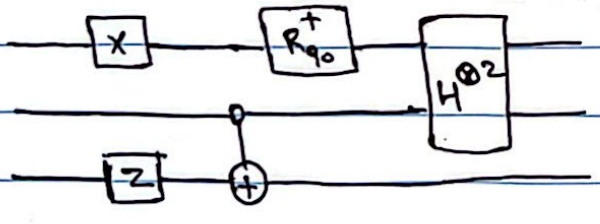
c) Write complete circuit as unitary matrix

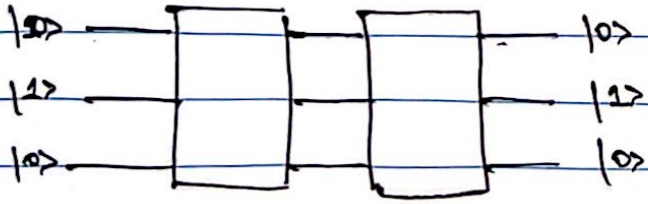
d) Write rererse circuit as unitary matrix

e) Compute output using unitary matrix of circuit.

Sol:-

a) In order to make rererse we have to make conjugate transpose of each the gates, But since most of the gates (except rotation) are harmission gates therefore no need to take conjugate transpose as $H^{\dagger} = H$





Foundation for Advancement of Science & Technology

b) $|\psi_1\rangle = |0\rangle |1\rangle |0\rangle$

$|\psi_2\rangle = H^{\otimes 2}(|0\rangle|1\rangle)|0\rangle$

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

$= \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2} \cdot |0\rangle$

$= \frac{|000\rangle-|010\rangle+|100\rangle-|110\rangle}{2}$

$R_{90} = \begin{pmatrix} \cos 90 & -\sin 90 \\ \sin 90 & \cos 90 \end{pmatrix}$

$|\psi_3\rangle = R_{90}|\psi_2\rangle$ $= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|0\rangle$

$= \frac{|100\rangle-|110\rangle-|000\rangle+|010\rangle}{2}$ $= |1\rangle$

$R_{90}|1\rangle = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

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

(CNOT)

$|\psi_3\rangle = \frac{|100\rangle-|111\rangle-|000\rangle+|011\rangle}{2}$

$|\psi_4\rangle = \frac{|000\rangle+|011\rangle-|100\rangle-|111\rangle}{2}$

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

Foundation for Advancement of Science & Technology

c) $S_1 = H \otimes H \otimes I$ (8×8)

$S_2 = R_{90} \otimes CNOT$ (8×8)

$S_3 = X \otimes I \otimes Z$ (8×8)

If nothing written in circuit parallel to a gate, add the identity gate. (I)

In what order should be multiply S_1, S_2 & S_3?

i) $S_1 \times S_2 \times S_3$ ✗

ii) $S_3 \times S_2 \times S_1$ ✓

Computing unitary matrix:

$$S_1 = H \otimes H \otimes I$$

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

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

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

Foundation for Advancement of Science & Technology

$S_2 = R_{90} \otimes CNOT$

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

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

$S_3 = X \otimes I \otimes Z$

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

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

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

$$S_3 \times S_2 \times S_1 = \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \end{pmatrix}$$

d) Conjugate Transpose of $S_3 \times S_2 \times S_1$ is the unitary matrix of the reverse circuit

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

e) Output $= \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 & 0 \\ -1 & 0 & -1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & -1 & 0 & 1 & 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

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

(Same as part b answer)

Foundation for Advancement of Science & Technology

Quantum Computing

Entanglement

1st def

① Given a state of multiple entangled qubits, one connot express individual qubits seperately

e.g

- $\frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$

There is no value of α, β, γ & δ, where left hand side = right hand side So we say these qubits are entangled.

- $\frac{|01\rangle + |00\rangle}{\sqrt{2}} = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

Above is an example of seperated. These qubits can be expressed separately. $\alpha = 1, \beta = 0, \gamma = \frac{1}{\sqrt{2}}$, & $\beta = \frac{1}{\sqrt{2}}$

2nd def

② Given a state of multiple entangled qubits, measuring any qubit individually reveals all other qubits.

e.g

Entangled

- $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ | Measure 1st qubit and 2nd
  - 1 → 1
  - 1/0 → 0
  - 2nd (M) 1st
  - 1/0 → 0
  - → 1

Separable

- $\frac{|01\rangle + |00\rangle}{\sqrt{2}}$ | 1st $|0\rangle$
  - 2nd
  - $|0\rangle - \frac{1}{2}$
  - $|1\rangle - \frac{1}{2}$

Foundation for Advancement of Science & Technology

Bell state (AKA EPR states):

There are 4 qubits defined as bell state:

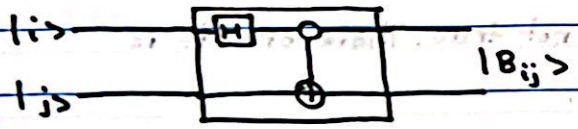
① $|\Phi^+\rangle = |B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

② $|\Phi^-\rangle = |B_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

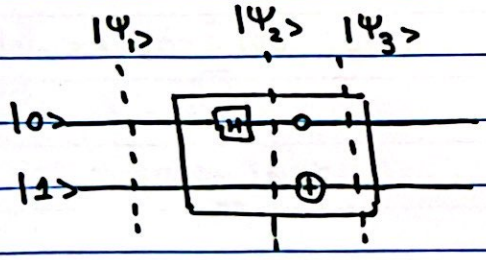
③ $|\Psi^+\rangle = |B_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

④ $|\Psi^-\rangle = |B_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$

→ Quantum circuit that creates Bell state:



e.g



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

$|\Psi_2\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}|1\rangle$

$= \frac{|01\rangle + |11\rangle}{\sqrt{2}}$

$|\Psi_3\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$

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

Foundation for Advancement of Science & Technology

e.g.

Q Given $|\omega\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$. Find if $|\omega\rangle$ is entangled or separable.

Sol:- Proof by contradiction

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \alpha|0\rangle + \beta|1\rangle \otimes \gamma|0\rangle + \delta|1\rangle$$

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

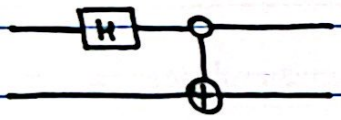
$$\alpha\gamma = 0,\ \alpha\delta = \frac{1}{\sqrt{2}},\ \beta\gamma = \frac{-1}{\sqrt{2}},\ \beta\delta = 0$$

$\downarrow$ either $\beta = 0$ or $\delta = 0$.

if $\beta = 0$, then $\beta\delta$ should be 0

& if $\delta = 0$, then $\alpha\delta$ " " ". But this is not true. Therefore it is entangled as LHS $\neq$ RHS.

⇒ How to create Bell states?



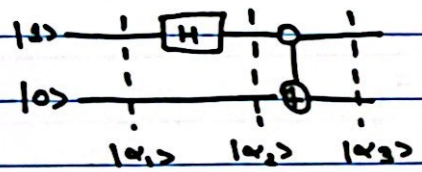
If input = $|x\rangle$ and $|y\rangle$.

$$|xy\rangle \longrightarrow \frac{|0y\rangle + (-1)^x |1\bar{y}\rangle}{\sqrt{2}}$$

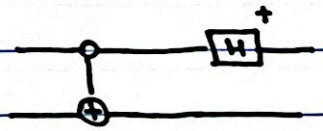
Foundation for Advancement of Science & Technology

	Input xy	Bell state	
i)	$\|00\rangle$	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$	$\|\Phi^+\rangle$
ii)	$\|01\rangle$	$\frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$	$\|\Psi^+\rangle$
iii)	$\|10\rangle$	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$	$\|\Phi^-\rangle$
iv)	$\|11\rangle$	$\frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$	$\|\Psi^-\rangle$

Verify $|10\rangle$,



Reverse circuit, $H^+ = H$



$|\alpha_1\rangle = |10\rangle$

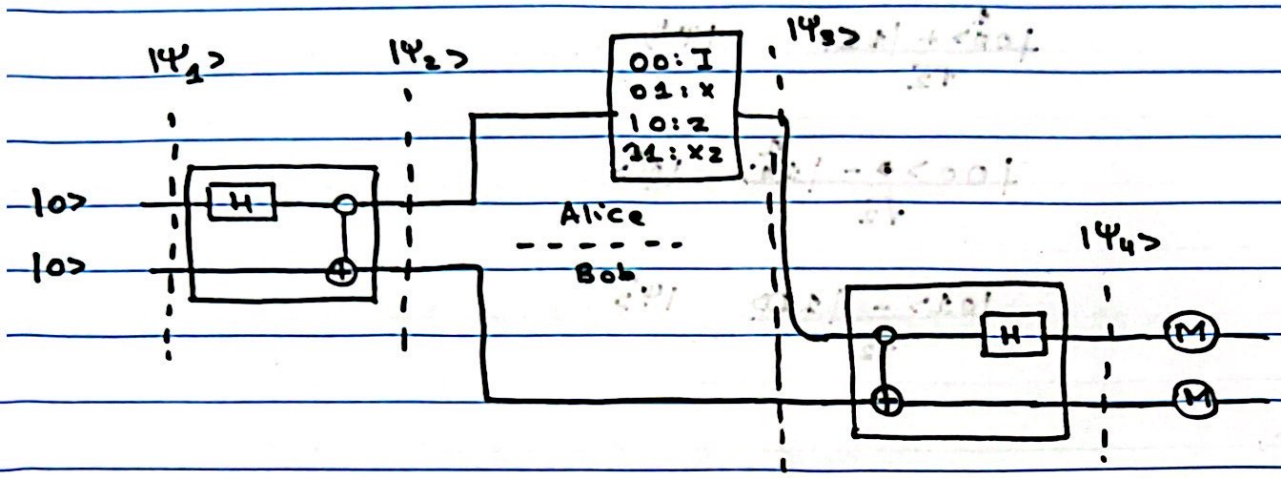
$|\alpha_2\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \cdot |0\rangle$

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

$|\alpha_3\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$

Foundation for Advancement of Science & Technology

Quantum Computing
Superdense Coding



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

$|\psi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

$|\psi_3\rangle$ depends on what Alice decides to send.

If Alice sends 00 $\Rightarrow |\psi_3\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

01: $|\psi_3\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}}$

10: $|\psi_3\rangle = Z|\psi_2\rangle$

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

11: $|\psi_3\rangle = X(Z|\psi_2\rangle)$

$= X\left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right)$

$= |10\rangle - |01\rangle / \sqrt{2}$

Foundation for Advancement of Science & Technology

$|\Psi_4\rangle$

Case 00: $|\Psi_4\rangle = CNOT\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$

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

$= H\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right)$ [only on 1st qubit]

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

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

$= \frac{2|00\rangle}{2} = |00\rangle$

Case 01: $|\Psi_4\rangle = CNOT\left(\frac{|10\rangle + |01\rangle}{\sqrt{2}}\right)$

$= \frac{|11\rangle + |01\rangle}{\sqrt{2}}$

$= H\left(\frac{|11\rangle + |01\rangle}{\sqrt{2}}\right)$

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

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

$= |01\rangle$

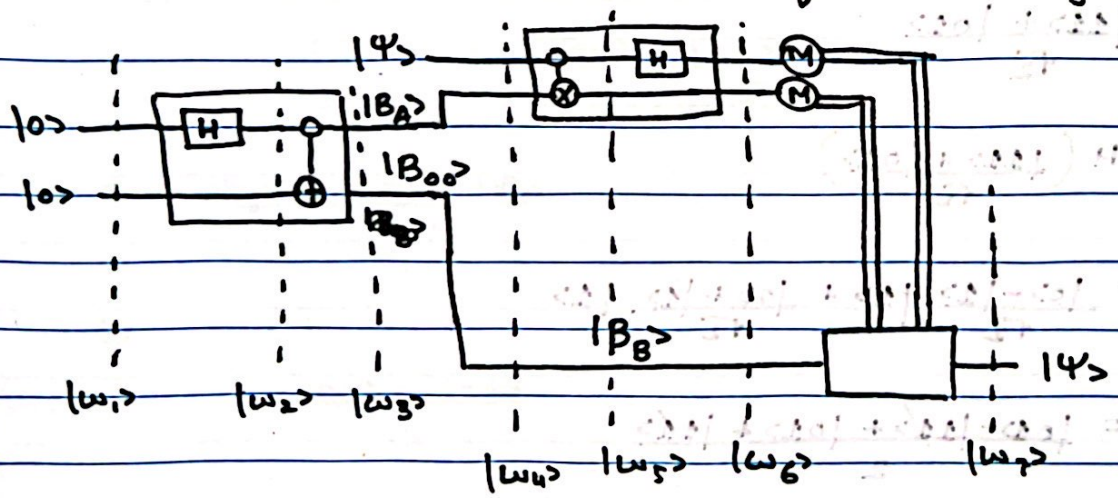
Case 10: $|\Psi_4\rangle = |10\rangle$

Case 11: $|\Psi_4\rangle = |11\rangle$

Foundation for Advancement of Science & Technology

Quantum Computing
Quantum Teleportation

Alice and Bob are two friends living together in New York. They get together & create a Bell state of 00 ($|B_{00}\rangle$). They then distribute the outcome of bell state among each other. Both of the qubits are entangled with each other. Portion Alice gets is $|B_A\rangle$ and likewise Bob gets $|B_B\rangle$. After some time Bob moves away from New York to Mars and Bob takes his portion of Bell state with him. After some time, Alice wishes to send a qubit ($|\psi\rangle$) while maintaining the secrecy of the qubit. Alice will perform operation on $|\psi\rangle$ and her portion of bell state qubit ($|\psi\rangle, |B_A\rangle$). Result of this operation is 2 classical bits (b_1 and b_2). Based upon the classical bits Bob will perform operations with his part of the bell state bit and retrieve the secret qubit sent by Alice.



Foundation for Advancement of Science & Technology

$|\omega_1\rangle = |0\rangle|0\rangle$

$|\omega_2\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot |0\rangle$

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

$|\omega_3\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |B_{00}\rangle$

$|\omega_4\rangle = |\psi\rangle \cdot |B_{00}\rangle$ $\qquad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$= (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right)$

$= \frac{\alpha|000\rangle + \alpha|100\rangle + \beta|100\rangle + \beta|110\rangle}{\sqrt{2}}$

$|\omega_5\rangle = \frac{\alpha|000\rangle + \alpha|100\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}$ $\qquad /\sqrt{2}$

$|\omega_6\rangle = \left[\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}\cdot|00\rangle + \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}}\cdot|11\rangle + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}\cdot|10\rangle + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}\cdot|01\rangle\right.$

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

$- \beta|0\rangle)$

$= \frac{1}{2}\left[|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |11\rangle(\alpha|1\rangle -\right.$

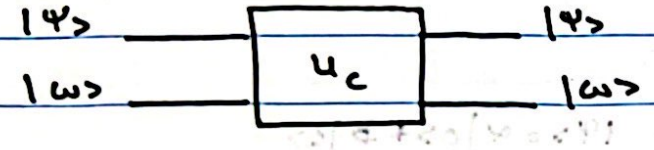
(M)	Prob	Resultant state	Operations Bob
00	1/4	$\alpha\|0\rangle + \beta\|1\rangle$	No operation
10	1/4	$\alpha\|0\rangle - \beta\|1\rangle$	$Z\|B_B\rangle = \alpha\|0\rangle + \beta\|1\rangle$
01	1/4	$\alpha\|1\rangle + \beta\|0\rangle$	$X\|B_B\rangle = \alpha\|0\rangle + \beta\|1\rangle$
11	1/4	$\alpha\|1\rangle - \beta\|0\rangle$	$Z(X\|B_B\rangle) = \alpha\|0\rangle + \beta\|1\rangle$

Foundation for Advancement of Science & Technology

Quantum Computing

No cloning Theorem

Theorem: There is no unitary operator U_c that can clone arbitrary qubits $|\psi\rangle$



$|\omega\rangle = |0\rangle$

$$\boxed{U_c|\psi\rangle|\omega\rangle = |\psi\rangle|\omega\rangle}$$

- All unitary operators must be linear

$$U_c(a|\psi\rangle + b|\phi\rangle)$$
$$= a U_c|\psi\rangle + b U_c|\phi\rangle$$

Proof 1:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$|\psi\rangle|0\rangle = \alpha|00\rangle + \beta|10\rangle$$
$$U_c(\alpha|00\rangle + \beta|10\rangle) = \alpha U_c|00\rangle + \beta U_c|10\rangle$$
$$(\alpha|00\rangle + \beta|10\rangle)(\alpha|00\rangle + \beta|10\rangle) \equiv \alpha|00\rangle\otimes|00\rangle + \beta|10\rangle\otimes|10\rangle$$
$$\alpha^2|0000\rangle + \alpha\beta|0010\rangle + \beta\alpha|1000\rangle + \beta^2|1010\rangle \equiv \alpha|0000\rangle + \beta|1010\rangle$$

LHS ≠ RHS

Not linear, hence cannot exist

Foundation for Advancement of Science & Technology

Proof a:

- Unitary operators preserve inner product of vectors

$$A|x\rangle = |m\rangle$$

$$A|y\rangle = |n\rangle$$

$$\langle x|y\rangle = \langle m|n\rangle$$

(Before operation) (After operation)

$$\Rightarrow U_c |\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

$$U_c |\theta\rangle|0\rangle = |0\rangle|0\rangle$$

$$(\langle\psi|\langle 0|)(|0\rangle|0\rangle) = (\langle\psi|\langle\psi|)(|\theta\rangle|0\rangle)$$

$$\langle\psi|\theta\rangle \cdot \underbrace{\langle 0|0\rangle}_{=1} = \langle\psi|0\rangle\langle\psi|0\rangle$$

$$\langle\psi|\theta\rangle = \langle\psi|0\rangle^2$$

Equal iff $\langle\psi|\theta\rangle = 1$ or 0.

inner product = 0 means orthogonal vectors

" " = 1 means same vectors

We can make a cloning machine for only 1 type of inner product

Foundation for Advancement of Science & Technology

Quantum Computing

Deutsch Algo

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

- This function would be either constant or balanced.
- constant means that for every input output would be same

x	f(x)
0	0
1	0

case 1

x	f(x)
0	1
1	1

case 2

- balanced states that one bit would be 1 and the other would be 0

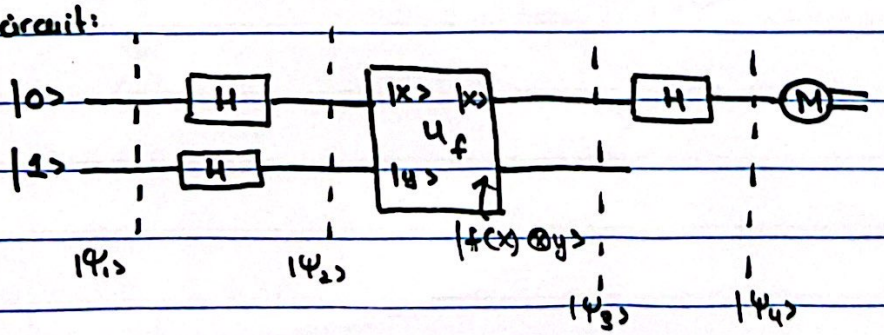
x	f(x)
0	0
1	1

case 3

x	f(x)
0	1
1	0

case 4

Quantum circuit:



Measure

if 0 (constant)

" 1 (balanced)

Foundation for Advancement of Science & Technology

Case 3:

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

$|\psi_2\rangle = |0\rangle|1\rangle$

$= |+\rangle|-\rangle$

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

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

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

$0 \oplus f(x) = f(x)$

$\therefore |x\rangle|y \oplus f(x)\rangle$

$|\psi_3\rangle = U_f |\psi_2\rangle$

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

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

Case 3:

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

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

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

$= |-\rangle|-\rangle$

$|\psi_4\rangle = H|-\rangle \cdot |-\rangle$

$= |1\rangle|-\rangle$

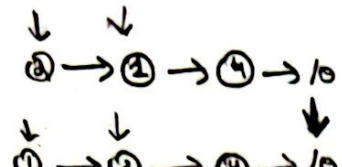
In $|\psi_3\rangle$,

constant: $|\psi_3\rangle = \pm|1\rangle|-\rangle$

as $H|+\rangle = |0\rangle$ so (M) $|0\rangle$

balanced: $|\psi_3\rangle = \pm|-\rangle|-\rangle$

$H|-\rangle = |1\rangle$ so (M) $|1\rangle$

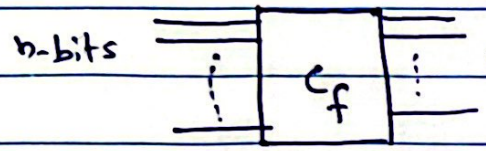


Quantum Computing

Classical Circuit to Quantum Circuit.

$f: \{0,1\}^n \rightarrow \{0,1\}^m$ ~ classical function

$\equiv$

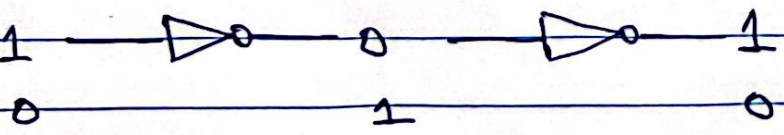


~ classical circuit

- Classical circuits are not inherently reversible, while quantum circuits must be reversible to comply with the principles of quantum mechanics
- Therefore to convert our initial classical circuit to quantum circuit, it has to undergo a transformation to become reversible

Universal gate set :- {AND, NOT}

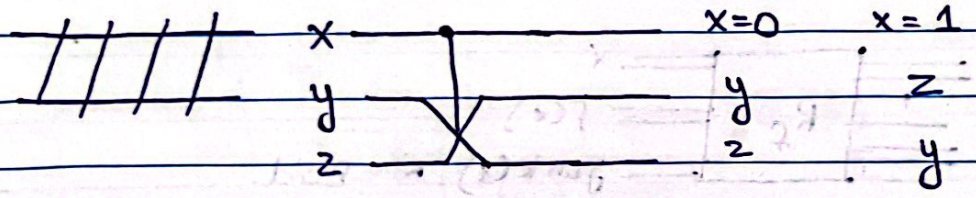
- All classical circuits can be drawn ONLY using AND & NOT
- Note that classical NOT gate already possesses the property of reversibility
- For instance, consider the operation of NOT gate. When we input 1 it produces 0 and if we pass this 0 through the NOT gate once more, it returns the original input & vice versa



Foundation for Advancement of Science & Technology

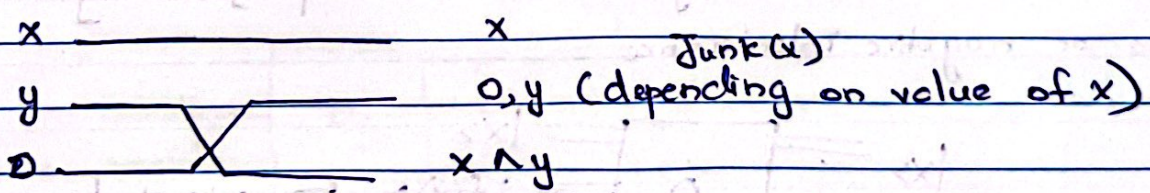
- But the classical AND gate is not reversible

- output 0 could be generated using 3 different combinations
- we cannot use the AND gate input to determine the exact original inputs. Thus AND gate is not reversible
- To create a reversible AND gate consider the Controlled-Swap (C-SWAP) gate



x: control bit for swapping.

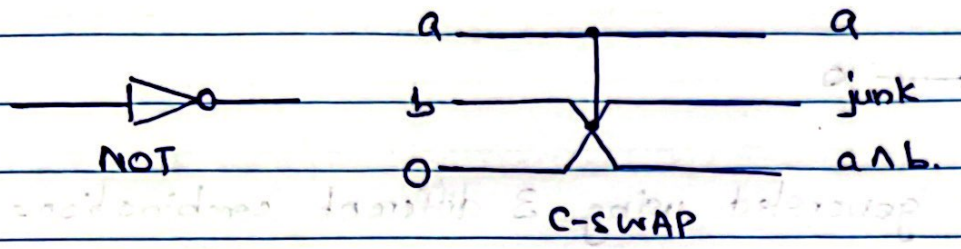
- To create an AND gate using the C-SWAP gate, we set z equal to zero.



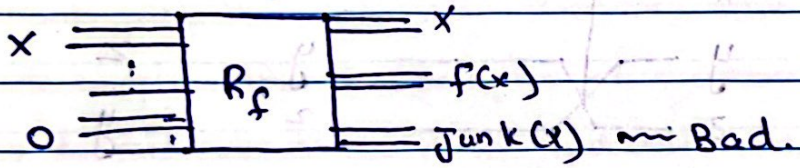
x	y	
0	0	0
0	1	0
1	0	y=0
1	1	y=1

Foundation for Advancement of Science & Technology

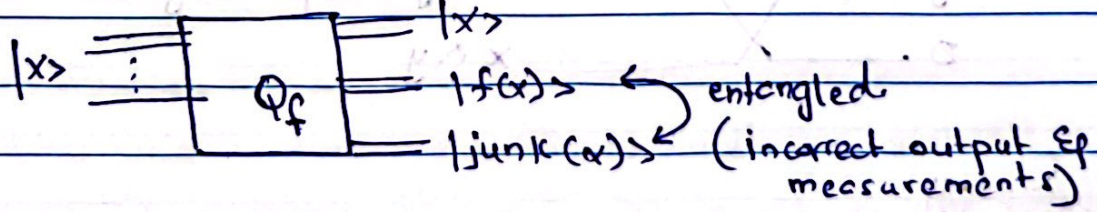
Universal set of reversible circuits:



• We can create a reversible circuit for function f, denoted by R_f using the reversible NOT & C-SWAP gate.



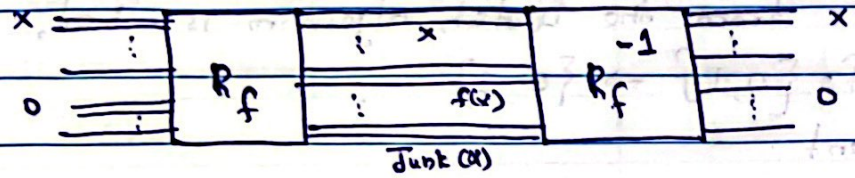
• The Junk could cause problems. If we convert a classical reversible circuit with this junk into a quantum circuit, lets call it Q_f, the junk could become entangled with the output, causing either positive or negative interference



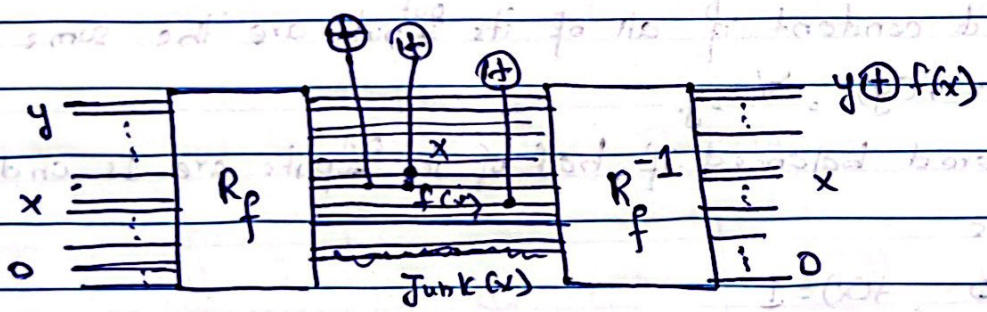
• Therefore we must modify our classical reversible circuit to eliminate this junk to ensure the quantum circuit functions correctly.

Foundation for Advancement of Science & Technology

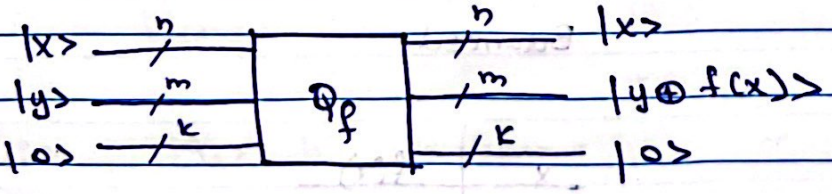
- To eliminate junk we feed the output of our classical circuit R_f into its inverse thus converting the output back to original input



- However, this process has also eliminated $f(x)$.
- To preserve the value of $f(x)$ we introduce controlled NOT (CNOT) gate



$\Rightarrow$



- For simplicity we can omit the $|0\rangle$ input & output

Foundation for Advancement of Science & Technology

Deutsch-Jozsa Algorithm
(Generalization of Deutsch Algorithm)

Problem Definition: Key difference from the Deutsch algorithm is that,

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

find f is constant

or

f is balanced?

→ Function is considered constant if all of its outputs are the same

$$f(x) = f(y), \forall x, y$$

→ Function is considered balanced if, half of its outputs are 1s and other half are 0s

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

for e.g. n: 2

Constant

x	f(x)
00	0 or 1
01	0 or 1
10	0 or 1
11	0 or 1

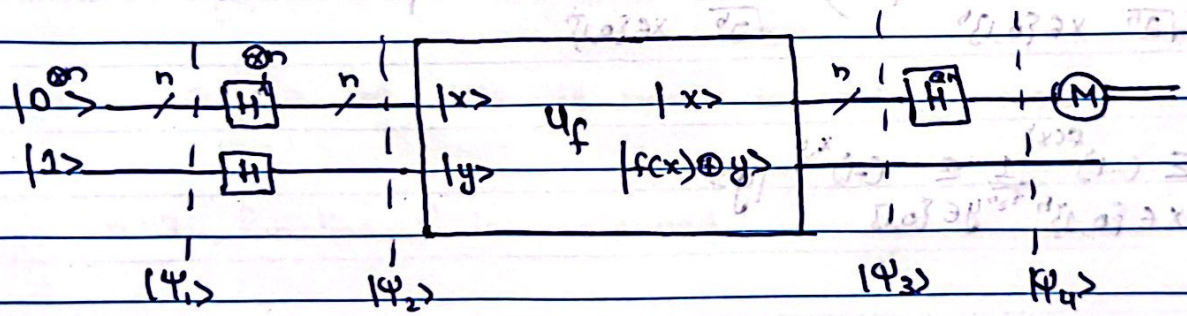
Balanced:

x	f(x)	
00	1	half 1s & half 0s
01	0	(any 2 inputs can
10	0	output 0 or 1s as
11	1	long as there are
		equal no of 1s and 0s)

Foundation for Advancement of Science & Technology

Classical	Quantum
• Must check one more than half of the total inputs. Thus, no of inputs to be examined is $(2^{n-1}+1)$ This implies a time complexity of $O(2^n)$ • If all are the same ⇒ constant otherwise ⇒ balanced	: Call oracle once via superposition. Time complexity : $O(1)$ • Exponential speedup

Quantum circuit for Deutsch-Jozsa Algorithm:-



$$|\psi_1\rangle = |0^n\rangle|1\rangle \quad , \quad |\psi_2\rangle = H^{\otimes n}|0^n\rangle\, H|1\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{|-\rangle}$$

Foundation for Advancement of Science & Technology

x	y	XOR
0	0	0
0	1	1
1	0	1
1	1	0

$|\psi_3\rangle = U_f |\psi_2\rangle$

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

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

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

$f(x) \oplus 0 = f(x)$

$f(x) \oplus 1 = f(\bar{x})$

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

$|\psi_4\rangle = H^{\otimes n}\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} H^{\otimes n} |x\rangle$

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

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

Case 1: f is constant. claim is that we can measure $|y\rangle$ as $|0^n\rangle$ with a prob of 1

- Fact #1: $x \cdot y = 0$
- " #2: $f(x)=0 \Rightarrow (-1)^{f(x)} = 1$ thus $|\psi_4\rangle = \frac{1+1+1+1+\ldots+1}{2^n} |0^n\rangle$

$= \frac{2^n}{2^n} |0^n\rangle$

$= |0^n\rangle$

• $f(x)=1 \Rightarrow (-1)^{f(x)} = -1$ thus $|\psi_4\rangle = \frac{-1-1-1+\ldots\ldots-1}{2^n}|0^n\rangle$

$$= \frac{-2^n}{2^n}|0^n\rangle = -|0^n\rangle$$

$\text{Prob} = (-1)^2 = 1$

⇒ In conclusion, when the function is constant for both $f(x)=0$ & $f(x)=1$ we will measure $y = |0\rangle$ with 100% prob.

Case 2: f is Balanced. Claim is that we will never measure $y=|0^n\rangle$

if $|y\rangle = |0^n\rangle \Rightarrow xy=0$

$f(x)=1$ half

$f(x)=0$ half

$$|\psi_4\rangle = \frac{2^{n-1}-2^{n-1}}{2^n}|0^n\rangle$$

$|\psi_4\rangle = 0|0^n\rangle \Rightarrow$ We will never be able to measure $|0^n\rangle$

e.g. $n=2$, function f is balanced

x	f(x)
00	1
01	0
10	0
11	1

(M) $\neq |0^n\rangle$

$|\psi_1\rangle = |00\rangle|1\rangle$, $|\psi_2\rangle = H^{\otimes 2}|00\rangle\, H|1\rangle$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^2}}\left[|00\rangle+|01\rangle+|10\rangle+|11\rangle\right]|-\rangle$$

$|\psi_3\rangle = U_f|\psi_2\rangle$ (Since the 2nd register has $|-\rangle$, U_f gate would change the sign of all inputs which have output = 1)

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

Foundation for Advancement of Science & Technology

$$|\psi_4\rangle = \frac{1}{2}\left[-H|00\rangle + H|01\rangle + H|10\rangle - H|11\rangle\right]$$

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$-\|00\rangle$	-	-	-	-
$\|01\rangle$	+	-	+	-
$\|10\rangle$	+	+	-	-
$-\|11\rangle$	-	+	+	-
	0	0	0	-4

x_1x_2	y_1y_2
	$(-1)^{x_1y_1+x_2y_2}$

$$|\psi_4\rangle = \frac{1}{2}\cdot\frac{1}{2}\left[-4|11\rangle\right] = -|11\rangle$$

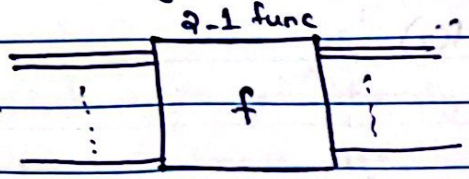
(M) $|11\rangle$ with prob $= (-1)^2 = 1$. Since y is not equal to $|00\rangle$ we can conclude that our function is balanced

Foundation for Advancement of Science & Technology

Quantum Computing
Simon's Algorithm

Problem Definition:

Given a 2-1 function $f: \{0,1\}^n \rightarrow \{0,1\}^n$, such that $f(x) = f(x \oplus s)$ for $s \in \{0,1\}^n$, our goal is to find s



s: secret message

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

e.g $n=3$, $s=101$ ← assign random outputs but don't repeat

domain x	range f(x)
000	111
001	000
010	110
011	010
100	000
101	111
110	010
111	110

x: 001
s: 101
xor: 100.

- In classical computers, we give different inputs to function f and observe corresponding outputs. when we have 2 inputs that have same output then we stop. We take XOR of inputs to find s.

$x, z \rightarrow y$

$x \oplus z = s$

domain = 2^n

half input i.e 2^{n-1} produce unique outputs. we have to try. $2^{n-1}+1$ inputs

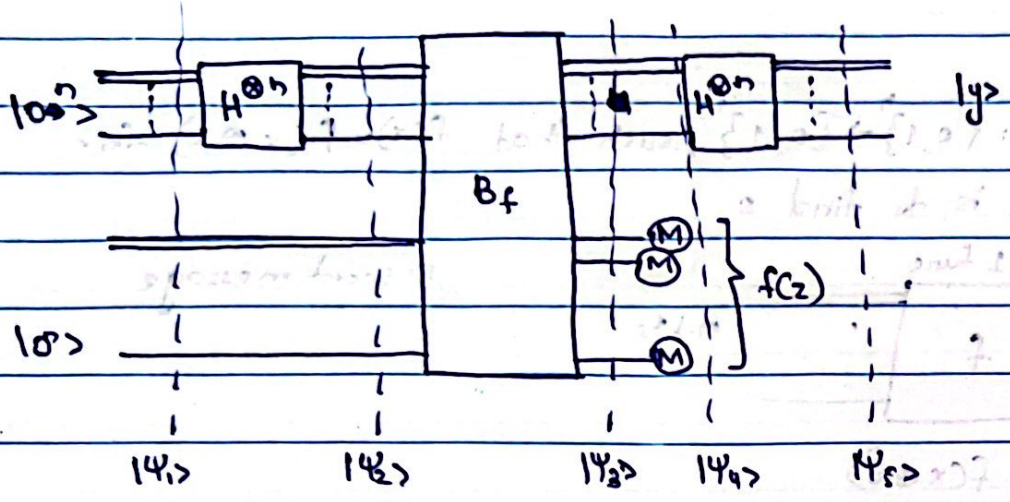
$\Rightarrow$ exponential time : $O(2^n)$. with randomized algo $\Rightarrow 2^{n/2}$: $O(2^n)$.

Quantum Algo : $O(n)$

Foundation for Advancement of Science & Technology

Quantum Computing

Circuit of Simons Algorithm



B_f : unitary wrapper over a 1-1 func

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

$$|\psi_2\rangle = H^{\otimes n} |0^n\rangle |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle$$

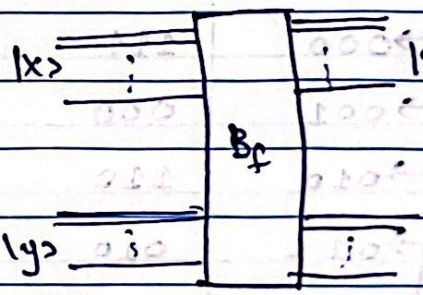
$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

$$|\psi_4\rangle = \frac{|z\rangle + |z \oplus s\rangle}{\sqrt{2}} |f(z)\rangle$$

$$|\psi_5\rangle = H^{\otimes n} \left(\frac{|z\rangle + |z \oplus s\rangle}{\sqrt{2}} \right) |f(z)\rangle$$

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

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



In our case, $|y\rangle = |0\rangle$

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

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

Foundation for Advancement of Science & Technology

$$|\psi_5\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot z} \left[1 + (-1)^{y \cdot s}\right] |y\rangle$$

Case 1: $y \cdot s = 1$

prob of $y \cdot s = 1 \Rightarrow 0$. (can never happen)

Case 2: $y \cdot s = 0$

2^{n-1}, goal is to get $n-1$ linearly independent values of y.

Using system of linear eqs we can solve $y \cdot s$ for s

EXAMPLE: $n = 4$

$$|\psi_1\rangle = |0^n\rangle |0^n\rangle = |0000\rangle |0000\rangle$$

$$|\psi_2\rangle = H^{\otimes 4} |0000\rangle |0000\rangle$$

$$= \frac{1}{4} \sum_{x \in \{0,1\}^4} |x\rangle |0000\rangle$$

$$= \frac{|0000\rangle + |0001\rangle + \ldots\ldots + |1111\rangle}{4} |0000\rangle$$

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

$$|\psi_3\rangle = \frac{1}{4} \sum_{x \in \{0,1\}} |x\rangle |f(x)\rangle$$

$$= \frac{1}{4} \left[|0000\rangle |1111\rangle + |0001\rangle |0001\rangle + |0010\rangle |1110\rangle + \ldots + |1111\rangle |1010\rangle \right]$$

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

$s = 1001$

Foundation for Advancement of Science & Technology

$|\psi_4\rangle = \frac{|z\rangle + |z \oplus s\rangle}{\sqrt{2}} |f(z)\rangle$ Assume we measured, 1010

$= \frac{|0110\rangle + |1111\rangle}{\sqrt{2}} \cdot |1010\rangle$

$|\psi_5\rangle = H^{\otimes 4} \left[\frac{|0110\rangle + |1111\rangle}{\sqrt{2}} \right]$

$= \frac{|0000\rangle - |0010\rangle - |0100\rangle + |0110\rangle + |1001\rangle - |1011\rangle - |1101\rangle + |1111\rangle}{\sqrt{2^3}}$

$\therefore y \cdot s \neq 1$ Ep $y \cdot s = 0$.

Check: $y \cdot s = 0$

$|0000\rangle \cdot |1001\rangle \stackrel{?}{=} 0$

$0.1 + 0.0 + 0.0 + 0.1 \stackrel{?}{=} 0$

$0 + 0 + 0 + 0 = 0$ ✓

$|1111\rangle \cdot |1001\rangle \stackrel{?}{=} 0$

$1.1 + 1.0 + 1.0 + 1.1 \stackrel{?}{=} 0$

$2 \stackrel{?}{=} 0$ (mod 2 calculations)

$0 = 0$ ✓

Goal: find 3 (n-1) linearly independent y. Null vector not L.I.

① $Y = |00000\rangle$

② $Y = |00010\rangle$ ✓

③ $Y = |01000\rangle$ (not multiple of the previous y in the set) LI ✓

④ $Y = |01100\rangle$ (Not LI i.e $|00010\rangle + |01000\rangle = |01100\rangle$) ✗

⑤ $Y = |10001\rangle$ ✓

linearly independent

$Y_1\ Y_2\ Y_3\ Y_4$

① $|00010\rangle$

② $|01000\rangle$

③ $|10001\rangle$

Foundation for Advancement of Science & Technology

$Y^1 \cdot S = 0 \Rightarrow Y^1_1 \cdot S_1 + Y^1_2 \cdot S_2 + Y^1_3 \cdot S_3 + Y^1_4 \cdot S_4 = 0$

$Y^2 \cdot S = 0 \Rightarrow Y^2_1 \cdot S_1 + Y^2_2 \cdot S_2 + Y^2_3 \cdot S_3 + Y^2_4 \cdot S_4 = 0$

$Y^3 \cdot S = 0 \Rightarrow Y^3_1 \cdot S_1 + Y^3_2 \cdot S_2 + Y^3_3 \cdot S_3 + Y^3_4 \cdot S_4 = 0$

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

$$\left[\begin{array}{cccc|c} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right] \quad R_3 \leftrightarrow R_1$$

$$\left[\begin{array}{cccc|c} \textcircled{1} & 0 & 0 & 1 & 0 \\ 0 & \textcircled{1} & 0 & 0 & 0 \\ 0 & 0 & \textcircled{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$S_4 = 01$, $S_3 = 0$, $S_2 = 0$, $S_1 + S_4 = 0$

$S_1 = -S_4$

$S_1 = -1 \mod 2$

$S_1 = 1$

$\Rightarrow S = S_1 S_2 S_3 S_4$

$S = 1001$ ✓

Foundation for Advancement of Science & Technology

Quantum Computing
Quantum Fourier Transform

Primitive roots of unity:

$z^n = 1$, z is $\mathbb{C}$

then n different sols/roots $\{\omega_n^0, \omega_n^1, \omega_n^2, \dots, \omega_n^{n-1}\}$ where

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

① ω_n^k lie on unit circle

$|\omega_n^k| = 1$

Proof:

$$|\omega_n^k| = \sqrt{\omega_n^{k*} \cdot \omega_n^k}$$
$$= \sqrt{e^{-2\pi i \frac{k}{n}} \cdot e^{2\pi i \frac{k}{n}}}$$
$$= \sqrt{e^0} = 1 \quad \checkmark$$

② ω_n^k is a periodic function.

$\omega_n^k = \omega_n^{k \bmod n}$

EXAMPLE:

Write all roots for $z^4 = 1$.

$\omega_4^4 = \omega_4^{4 \bmod 4 = 0} = 1$

$\omega_4^7 = \omega_4^{7 \bmod 4 = 3} = -i$

$e^{\frac{\pi}{2}i} = i$, $e^{\pi i} = -1$, $e^{0i} = 1$, $e^{\frac{3}{2}\pi i} = -i$

$\Rightarrow \{\omega_4^0, \omega_4^1, \omega_4^2, \omega_4^3\}$

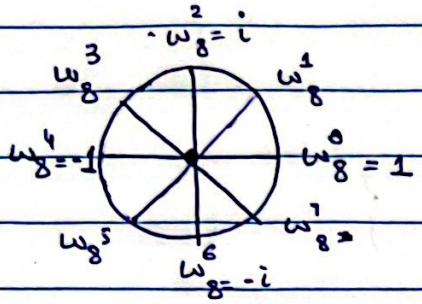
$= \{e^{2\pi i \frac{0}{4}}, e^{2\pi i \frac{1}{4}}, e^{2\pi i \frac{2}{4}}, e^{2\pi i \frac{3}{4}}\}$

$= \{e^{0i}, e^{\frac{\pi}{2}i}, e^{\pi i}, e^{\frac{3}{2}\pi i}\}$

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

Foundation for Advancement of Science & Technology

Q. Write all roots of $z^8 = 1$



$$\frac{360}{8} = 45.$$

$$\{1, \omega_8^1, i, i\omega_8, -1, -\omega_8, -i, -i\omega_8\}$$

- Discrete transformation matrix is a $n \times n$ matrix whose j^{th} col & k^{th} row element is equal to ω_n^{jk}. Rows & cols are counted from 0 instead of 1

$$F_n = \frac{1}{\sqrt{n}} \begin{pmatrix} \omega_n^{0\times0} & \omega_n^{0\times1} & \omega_n^{0\times2} & \cdots & \omega_n^{0\times(n-1)} \\ \vdots & & & & \\ \omega_n^{k\times0} & \omega_n^{k\times1} & \omega_n^{k\times2} & \cdots & \omega_n^{k\times(n-1)} \\ \vdots & & & & \\ & & & & \omega_n^{(n-1)(n-1)} \end{pmatrix}$$

$$= \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_n & \omega_n^2 & \omega_n^3 & \omega_n^{(n-1)} \\ 1 & \omega_n^2 & \omega_n^4 & \omega_n^6 & \omega_n^{2(n-1)} \\ 1 & \omega_n^3 & \omega_n^6 & \omega_n^9 & \omega_n^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cdots & \cdots & \cdots & \omega_n^{(n-1)(n-1)} \end{pmatrix}$$

row #0, #1, #2, #3, ..., #n-1

Foundation for Advancement of Science & Technology

Example:

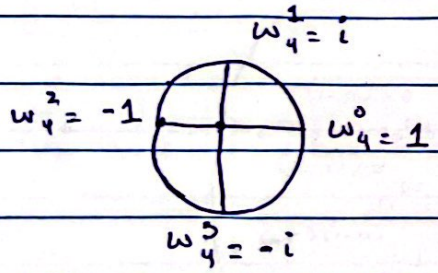
Q. Tranform $|\psi\rangle = \frac{|0\rangle + |3\rangle}{\sqrt{2}}$ using F_4

$F_4|\psi\rangle = |0\rangle$

$$\Rightarrow F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4^1 & \omega_4^2 & \omega_4^3 \\ 1 & \omega_4^2 & \omega_4^4 & \omega_4^6 \\ 1 & \omega_4^3 & \omega_4^6 & \omega_4^9 \end{pmatrix}$$

- To change ω values to actual numbers use unit circle

ω_4 : circle to be divided into 4 equal parts
i.e if $n=8$, 8 equal parts
& so on



$\omega_4^{4 \bmod 4} = \omega_4^0$

$\omega_4^{6 \bmod 4} = \omega_4^2$

$\omega_4^{3 \bmod 4} = \omega_4^1$

$$F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

$$|Q\rangle = F_4|\psi\rangle = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \begin{matrix} \leftarrow 0 \text{ row} \\ \leftarrow 1 \quad " \\ \leftarrow 2 \quad " \\ \leftarrow 3 \quad " \end{matrix}$$

$$= \frac{1}{2\sqrt{2}} \begin{pmatrix} 1+1 \\ 1-i \\ 1-1 \\ 1+i \end{pmatrix} = \frac{1}{2\sqrt{2}} \begin{pmatrix} 2 \\ 1-i \\ 0 \\ 1+i \end{pmatrix}$$

$$|Q\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1-i}{2\sqrt{2}}|1\rangle + \frac{1+i}{2\sqrt{2}}|3\rangle$$

- QFT does not provide complete matrix but is a sort of sampling of our output

Properties of Discrete Fourier Transformation (DFT):-

① DFT is unitary.

Proof:

$$\langle \vec{c_j} | \vec{c_k} \rangle = \begin{cases} 0 & j \neq k \text{ (orthogonal)} \\ 1 & j = k \text{ (normalized)} \end{cases}$$

$$\vec{c_i} = \frac{1}{\sqrt{n}} \begin{pmatrix} \omega^{0\times j} \\ \omega^{1\times j} \\ \omega^{2\times j} \\ \vdots \\ \omega^{(n-1)j} \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 \\ \omega^{j} \\ \omega^{2j} \\ \omega^{3j} \\ \vdots \\ \omega^{(n-1)j} \end{pmatrix}$$

Foundation for Advancement of Science & Technology

$$\vec{c}_k = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 \\ \omega^k \\ \omega^{2k} \\ \omega^{3k} \\ \vdots \\ \omega^{(n-1)k} \end{pmatrix}$$

Geometric Series:

$a + ra + r^2a + \dots + r^{n-1}a$

$\text{Sum}(S) = \frac{a(r^n - 1)}{r - 1}$ $\quad \boxed{\begin{matrix} a = 1 \\ r = \omega^{k-j} \end{matrix}}$

conjugate

$$\langle c_j | c_k \rangle = \frac{1}{n} \sum_{m=0}^{n-1} \omega^{\overline{mxj}} \cdot \omega^{mxk}$$

$$= \frac{1}{n} \sum_{m=0}^{n-1} \omega^{m(k-j)}$$

Case 1:- $\boxed{j = k}$

$$\langle c_j | c_k \rangle = \frac{1}{n} \sum_{m=0}^{n-1} \omega^0$$

$$= \frac{1}{n} [1 + 1 + \dots + 1] = \frac{n}{n} = \boxed{1}$$

Case 2: $\boxed{j \neq k}$

$$\langle c_j | c_k \rangle = \frac{1}{n} \sum_{m=0}^{n-1} \omega^{(k-j)}$$

$$= \frac{\omega^{(k-j)n} - 1}{\omega^{k-j} - 1}$$

$\therefore \omega_n^{fn} = 1 \Rightarrow \omega_n^{fn} = \omega_n^{fn \bmod n} = \omega_n^0 = 1$

$$= \frac{1 - 1}{\omega^{k-j} - 1} = \boxed{0}$$

Foundation for Advancement of Science & Technology

② Convolution ↔ Multiplication :-

$$\frac{1}{\sqrt{n}} \begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix}_{\text{DTF}} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}_{\text{Input vector}} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{n-1} \end{pmatrix}_{\text{Output vector}}$$

Measure output:

$|k\rangle \rightarrow |\beta_k|^2$ prob↑

linearly shift by 1

$$\begin{pmatrix} \alpha_{n-1} \\ \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-2} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \omega\,\beta_1 \\ \omega^2\beta_2 \\ \vdots \\ \omega^{n-1}\beta_{n-1} \end{pmatrix}$$

phase shift

Measure:

$|k\rangle \rightarrow |\beta_k|^2$

because

$|\omega^2| = |\omega^3| = 1.$

- If input has linear shift we can apply quantum fourier transformation and make sure that there is no shift in measurement

Proof:-

Before linear shift :- (k^{th} output)

$$\beta_k = \alpha_0 + \omega^k \alpha_1 + \omega^{2k} \alpha_2 + \dots\dots + \omega^{(n-1)k} \alpha_{n-1}$$

→ Output remains same after linear shift. Only a phase is attached to it which is ignored

Linear shift by 1 :-

$$\alpha_m = \alpha_{m+1}$$

$$\alpha_{n-1} + \omega^k \alpha_0 + \omega^{2k} \alpha_1 + \omega^{3k} \alpha_2 + \dots + \omega^{(n-1)k} \alpha_{n-2}$$

[k^{th} output After Linear shift]

$$\omega^k \beta_k = \omega^k \alpha_0 + \omega^{2k} \alpha_1 + \omega^{3k} \alpha_2 + \dots\dots + \omega^{nk} \alpha_{n-1}$$

$$= \quad " \quad " \quad " \quad + \omega^0 \alpha_{n-1}$$

$nk \bmod n = 0$

Foundation for Advancement of Science & Technology

⑨ Period / wavelength relationship :-

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

QFT is same as DFT

$$\begin{pmatrix} QFT \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{r-1} \\ \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{\frac{N}{r}-1} \\ \beta_0 \\ \beta_1 \end{pmatrix}$$

QFT $f(x) = \hat{f}(x)$

if period = r then $\frac{N}{r} = \frac{2^n}{r}$

Periodic Finding Algorithm

Problem Definition : Given a periodic function $f: \{0,1\}^n \rightarrow \{0,1\}^n$, find period r, such that $f(x) = f(x + kr)$, $\forall\ k \in \mathbb{Z} - \{0\}$

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

$f(x) = x \bmod 3$

$n = 4$

x	f(x)
0	0
1	1
2	2
3	0
4	1
5	2
6	⋮
7	
8	
9	
10	
11	
12	
13	
14	
15	

Q. How can this problem be solved on a classical computer?

→ We can give diff inputs and find which 2 inputs yield the same output

$f(0) = 0$ ←

$f(1) = 1$

$f(2) = 2$

$f(3) = 0$ ←

$r = |3 - 0| = 3$

T.C = $\Theta(r)$

Generally: T.C = $\Theta(2^n)$

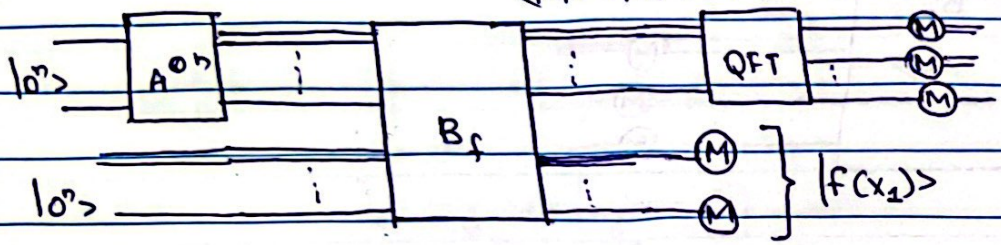
- QFT removes the linear shift from the input. It will have a phase shift, but since phase shift does not effect the result of measurement, we can achieve our speed up
- QFT also changes the period of a function

In below case :- Before QFT: period $= r$, After QFT: period $= \frac{2^n}{r}$

- We would have to first develop a quantum wrapper over the function f to use it

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

$$\left(|x_1\rangle + |x_1+r\rangle + |x_1+2r\rangle + \ldots + |x_1+\left(\tfrac{2^n}{r}-1\right)r\rangle\right)/\sqrt{2^n/r}$$



B_f

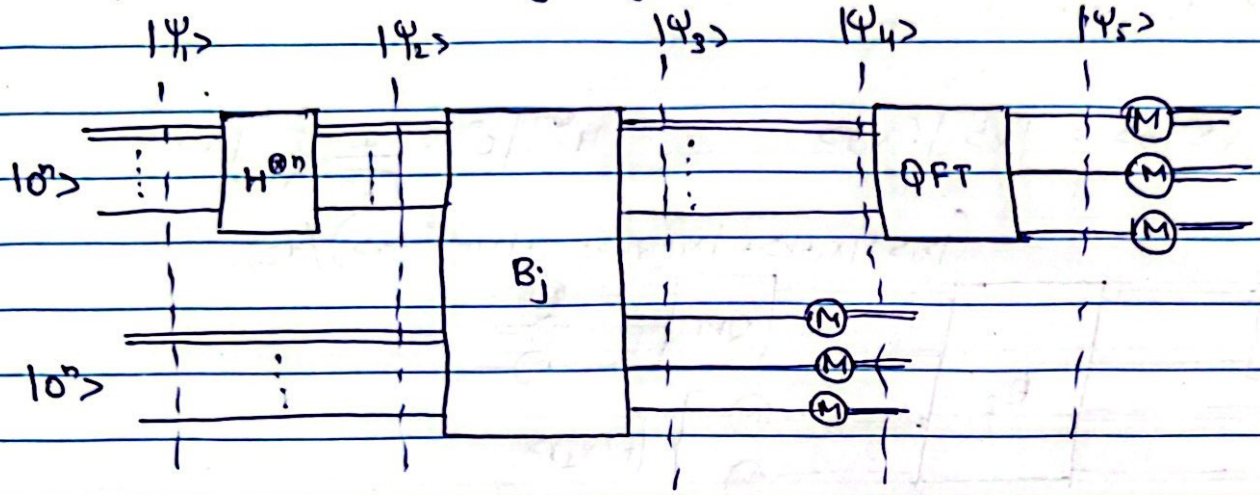
1st register: $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$ (All possible values of x in superposition)

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

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

2nd register measured	First register superposition
$\|f(0)\rangle$	$\|0\rangle + \|0+r\rangle + \|0+2r\rangle + \ldots\ldots$
	L.S (Linear shift)
$\|f(1)\rangle$	$\|1\rangle + \|1+r\rangle + \|1+2r\rangle + \ldots\ldots$
$\|f(2)\rangle$	$\|2\rangle + \|2+r\rangle + \|2+2r\rangle + \ldots\ldots$
$\|f(k)\rangle$	$\|k\rangle + \|k+r\rangle + \|k+2r\rangle + \ldots\ldots$

Example of Period Finding Algorithm :-



Example: find period r given $f: \{0,1\}^3 \rightarrow \{0,1\}^3$ [For use in B_f ⇒ $f(x) = x \bmod 2$

↑ for any even number $f(x) = 0$ & for odd number ~~it would be~~ $f(x) = 1$

Sol:-

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

$$|\psi_2\rangle = H^{\otimes 3}|000\rangle\,|000\rangle$$

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

$$= \frac{|0\rangle + |1\rangle + |2\rangle + \ldots + |7\rangle}{\sqrt{2^3}} \cdot |000\rangle$$

$$|\psi_3\rangle = B_f\,|\psi_2\rangle$$

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

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

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

Foundation for Advancement of Science & Technology

- Assume that we measure $|1\rangle$ in 2nd register

$$|\psi_4\rangle = \frac{(|1\rangle + |3\rangle + |5\rangle + |7\rangle)}{\sqrt{4}} |1\rangle \quad — ①$$

- Assume that we measure $|0\rangle$ in 2nd register

$$|\psi_4\rangle = \frac{(|0\rangle + |2\rangle + |4\rangle + |6\rangle)}{\sqrt{4}} |0\rangle \quad — ②$$

↙ only first register ①

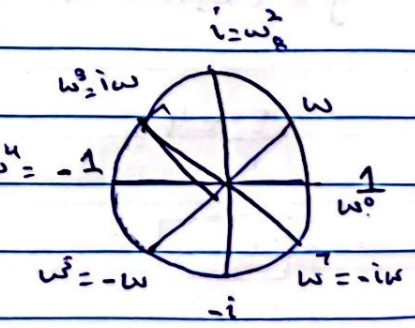
$$|\psi_5\rangle = QFT_8 \, |\psi_4\rangle$$

first possibility ↑

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

$$= \frac{1}{4\sqrt{2}} \begin{pmatrix} 1+1+1+1 \\ \omega_8^1 + \omega^3 + \omega^5 + \omega^7 \\ \omega^2 + \omega^6 + \omega^{10} + \omega^{14} \\ \omega^3 + \omega^9 + \omega^{15} + \omega^{21} \\ \omega^4 + \omega^{12} + \omega^{20} + \omega^{28} \\ \omega^5 + \omega^{15} + \omega^{25} + \omega^{35} \\ \omega^6 + \omega^{17} + \omega^{30} + \omega^{42} \\ \omega^7 + \omega^{21} + \omega^{35} + \omega^{49} \end{pmatrix} = \frac{1}{4\sqrt{2}} \begin{pmatrix} 4 \\ 0 \\ 0 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$= \frac{|0\rangle - |4\rangle}{\sqrt{2}}$$



Foundation for Advancement of Science & Technology

Measure $|\psi_5\rangle$

$|0\rangle$ with prob $= \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

$|4\rangle$ with prob $= \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$

- If we would have used $|\psi_4\rangle = \frac{|0\rangle + |2\rangle + |4\rangle + |6\rangle}{\sqrt{4}} \cdot |0\rangle$

This would yield some result but with different phase shift

$$|\psi_5\rangle = \frac{|0\rangle + |4\rangle}{\sqrt{2}}$$

rerun $O(\log N) = O(\log 2^3)$

save measurements.

Then take gcd of our measurements we will get $\frac{N}{r}$

$\gcd(0,4) = 4$

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

$$\boxed{r = 2}$$

Foundation for Advancement of Science & Technology

Roots of Unity

$$z^n = 1$$

$$\{ \omega_n^0, \omega_n^1, \omega_n^2, \omega_n^3, \ldots\ldots, \omega_n^{n-1} \}$$

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

e.g roots of $z^3 = 1$

$$\{ \omega_3^0, \omega_3^1, \omega_3^2 \}$$

$$\omega_3^0 = e^{2\pi i \frac{0}{3}} = 1$$

$$\omega_3^1 = e^{2\pi i \frac{1}{3}} \neq$$

$$\omega_3^2 = e^{2\pi i \frac{2}{3}} \neq$$

① Exponential Form:

$$\{ 1, e^{2\pi i/3}, e^{4\pi i/3} \}$$

$$re^{i\theta}$$

② Modulus-Argument Form:

$$z = r\cos\theta + ri\sin\theta$$

$$\{ 1, \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right), \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) \}$$

③ Cartesian Form:

$$\{ 1, -\frac{1}{2} + i\frac{\sqrt{3}}{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2} \}$$

Foundation for Advancement of Science & Technology

Example: $z^3 = 8$. Find roots

Sol: $z = \sqrt[3]{8}$

$= 2$

Exponential Form: $\{ 2, 2e^{\frac{2\pi}{3}i}, 2e^{\frac{4\pi}{3}i} \}$

Cartesian Form: $\{ 2, -1 + i\sqrt{3}, -1 - i\sqrt{3} \}$

Example: $(z-5)^3 = 8$. find roots

Sol: let $z - 5 = y$

$y^3 = 8$

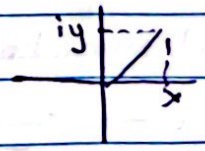
$\{ 2, -1 + i\sqrt{3}, -1 - i\sqrt{3} \}$

$z = y + 5$

$\{ 7, 4 + i\sqrt{3}, 4 - i\sqrt{3} \}$

Modulus - Argument Form.

Cartesian Form: $z = x + iy$ ⟶ modulus - argument ⟶ $z = r\cos\theta + ir\sin\theta$



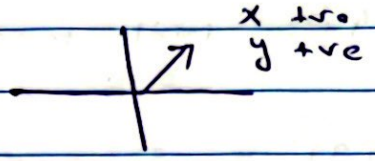
Modulus (magnitude): $|z| = \sqrt{x^2 + y^2}$

Argument: (Principle argument)

$-\pi < \theta \leq \pi$

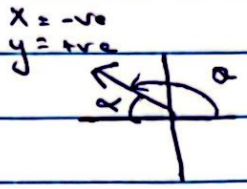
Foundation for Advancement of Science & Technology

Case 1: 1st quadrant



$$\theta = \tan^{-1}\left(\frac{y}{x}\right)$$

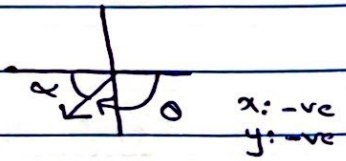
Case 2: 2nd quadrant



$$\alpha = \tan^{-1}\left|\frac{y}{x}\right|$$

$$\theta = \pi - \alpha$$

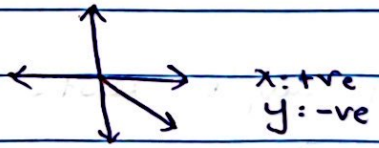
Case 3: 3rd quadrant



$$\alpha = \tan^{-1}\left|\frac{y}{x}\right|$$

$$\theta = -\pi + \alpha$$

Case 4: 4th quadrant



$$\alpha = \tan^{-1}\left|\frac{y}{x}\right|$$

$$\theta = -\alpha$$

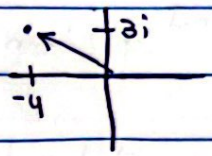
Foundation for Advancement of Science & Technology

Example: $z = -4+3i$, Write modulus-argument form

Sol)

$|z| = \sqrt{(-4)^2+(3)^2} = 5$ = radius.

$\alpha = \tan^{-1}\left|\frac{y}{x}\right|$



$\theta = \pi - \alpha$

$\theta = \pi - \tan^{-1}\left|\frac{3}{-4}\right|$

$\theta = 2.49$ rad

$\Rightarrow z = r\cos\theta + ir\sin\theta$

$= 5\cos(2.49) + i\sin(2.49)$

Exponential Form:-

cortesian form	Mod-arg form	exp form
$z = x+iy$	$z = r\cos\theta + ir\sin\theta$	$z = re^{i\theta}$

exp form : $5e^{i2.49}$

Solving eqs Ep complex roots:-

$ax^2+bx+c=0$

$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

Case 1: $b^2-4ac>0$

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

$\alpha \neq \beta$

Case 2: $b^2-4ac=0$

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

$\alpha = \beta$

Case 3: $b^2-4ac<0$

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

$\beta = \alpha^*$

Example: $x^2+2x+2=0$. find roots

$b^2-4ac = 4-4(1)(2) = 4-8 = -4$ (Case 3).

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{-2 \pm \sqrt{4-8}}{2} = \frac{-2 \pm \sqrt{-4}}{2} = \frac{-2 \pm 2i}{2} = -1 \pm i$$

Poly deg 3:

$ax^3+bx^2+cx+d=0 \quad a \neq 0$

① 3 real root

② 1 real, 2 complex roots

Poly deg 4:

① 4 real root

② 2 real root, 2 complex roots

③ 4 complex root $\alpha, \alpha^*, \beta, \beta^*$

e.g $z^4+13z^2+36=0$. Given $z=2i$ is a root. find remaining 3 roots

Sol).

$z=2i$, $z=-2i$

Factor: $(z-2i)(z+2i) = z^2-(2i)^2 = z^2+4$

$$z^2+4 \;\big)\; z^4+13z^2+36 \;\big(\; z^2+9$$

$$-(z^4+4z^2)$$

$$9z^2+36$$

$$-(9z^2+36)$$

$$0$$

$(z^2+4)(z^2+9)=0$

$z^2+9=0$

$z^2=-9$

$z=\pm\sqrt{-9} = \pm 3i$

Foundation for Advancement of Science & Technology

Arithmetic Operation :-

$$z_1 = a+ib, \quad z_2 = c+id$$

Addition / Subtraction :

$$z_1 + z_2 = (a+c) + i(b+d)$$

$$z_1 - z_2 = (a-c) + i(b-d)$$

Multiplication :

$$z_1 \cdot z_2 = (ac-bd) + i(ad+bc)$$

Division :

$$z_1 / z_2 = \frac{ac+bd+i(bc-ad)}{c^2+d^2}$$

$$\Rightarrow z_1 = r_1 e^{i\theta_1}, \quad z_2 = r_2 e^{i\theta_2}$$

Add / Sub :

$$z_1 + z_2 = r_1 e^{i\theta_1} + r_2 e^{i\theta_2}$$

Multiplication :

$$z_1 \cdot z_2 = r_1 \cdot r_2 \, e^{i\theta_1 + i\theta_2} = r_1 r_2 \, e^{i(\theta_1+\theta_2)}$$

Division :

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\theta_1-\theta_2)}$$

Foundation for Advancement of Science & Technology

4 result

① $\arg(z_1 z_2) = \theta_1 + \theta_2 = \arg(z_1) + \arg(z_2)$

② $\arg\left(\frac{z_1}{z_2}\right) = \theta_1 - \theta_2 = \arg(z_1) - \arg(z_2)$

③ $\left|\frac{z_1}{z_2}\right| = \frac{r_1}{r_2} = \frac{|z_1|}{|z_2|}$

④ $|z_1 z_2| = r_1 r_2 = |z_1| \cdot |z_2|$

Square root of complex numbers:

Q. Find square root of $7 + i6\sqrt{2}$

Soln

$$x+iy = \sqrt{7 + i6\sqrt{2}}$$

$$(x+iy)^2 = 7 + i6\sqrt{2}$$

$$x^2 + 2ixy - y^2 = 7 + i6\sqrt{2}$$

$$(x^2 - y^2) + i(2xy) = 7 + i6\sqrt{2}$$

$\Rightarrow x^2 - y^2 = 7 \quad -①$ $\qquad 2xy = 6\sqrt{2} \quad -②$

$$x^2 - \left(\frac{3\sqrt{2}}{x}\right)^2 = 7 \qquad xy = 3\sqrt{2}$$

$$y = \frac{3\sqrt{2}}{x}$$

$$x^2 - \frac{18}{x^2} = 7$$

$$y = \frac{3\sqrt{2}}{3} \qquad y = \frac{3\sqrt{2}}{-3}$$

$$x^4 - 18 = 7x^2$$

$$x^4 - 7x^2 - 18 = 0$$

$\boxed{y = \sqrt{2}}$ $\qquad \boxed{y = -\sqrt{2}}$

$u = x^2$

$$u^2 - 7u - 18 = 0 \qquad x^2 = 9 \qquad x^2 = -2$$

$$u = -7 \pm \sqrt{121}/2 \qquad \boxed{x = \pm 3} \qquad x$$

$$= 7 + 11/2 \qquad = 7 - 11/2$$

$3 + i\sqrt{2}$

$-3 - i\sqrt{2}$

Foundation for Advancement of Science & Technology

Finding square root using De Moivre's formula:

$z = r\cos\theta + ir\sin\theta$

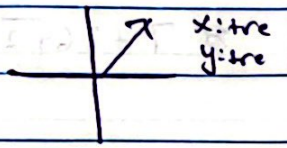
$z^n = r^n\cos(n\theta) + ir^n\sin(n\theta)$

$z^{1/2} = \sqrt{r}\cos\left(\frac{\theta}{2}\right) + i\sqrt{r}\sin\left(\frac{\theta}{2}\right)$

Q. find square root of $7 + i6\sqrt{2}$

$$|z| = r = \sqrt{7^2 + (6\sqrt{2})^2}$$
$$= \sqrt{49 + 72}$$
$$= \sqrt{121} = 11$$

$$\theta = \tan^{-1}\left|\frac{6\sqrt{2}}{7}\right| = 0.88 \text{ rad}$$



$$z^{1/2} = \sqrt{11}\cos\left(\frac{0.88}{2}\right) + i\sqrt{11}\sin\left(\frac{0.88}{2}\right)$$
$$= 3 + i\sqrt{2}$$

$$z^{1/2} = \sqrt{11}\cos\left(\frac{0.88 + 2\pi}{2}\right) + i\sqrt{11}\sin\left(\frac{0.88 + 2\pi}{2}\right)$$

$$= -3 - i\sqrt{2}$$

Foundation for Advancement of Science & Technology

RSA (asymmetric also) → public/private key

- RSA
- Shor

Sender (Alice)	Oscar (Hacker)	Receiver (Bob)
	$e=3, n=33, y=8$	Key generation:
Encryption:-	problem solve $n=p \times q$	• p, q prime numbers
plaintext: $x=2$	$n=3 \times 11$	$p=3, q=11$
$y=2^3 \bmod 33$	$\phi(n)=(3-1)\times(11-1)=20$	• $n=p \times q=33$
$=8$	$3.d=1 \bmod 20$	• $\phi(n)=(3-1)(11-1)=20$
totient function	$d=7 \quad (e,n)=(3,33)$	• public key e $\gcd(e, \phi(n))=1$
Euler phi function	$8^7 \bmod 33=2$	• $e=3$.
	$y=8$	• private key d: $d \times e \equiv 1 \bmod \phi(n)$
		$d=7$

Decryption:

$x = y^d \bmod n$

$= 8^7 \bmod 33 = (2)$

FAW

Foundation for Advancement of Science & Technology

N

Quantum Computing
Shor's Factorization Algorithm

- Given a number n which is composed of 2 prime numbers say u and v. Shor's Algorithm find prime ~~nos~~ factors of number n in polynomial time.
- In contrast if we have to find prime factors of a number n then on a classical computer it takes exponential time. Therefore, on classical computers we are able to use famous cryptography algo known as RSA.
- RSA security is based upon a one-way function which is integer factorization. And bcz Shor Algorithms can find integer factorization in a polynomial time so RSA will be nullified or will be useless when a fully powered/working quantum computer is realized

1) Background :-

- Modulus :

$20 \equiv 2 \pmod 3$

$2 \equiv 20 \pmod 3$

$20 \bmod 3 \equiv 2$

- Divisibility :

if $a \equiv 0 \bmod N$ then N/a

$32 \equiv 0 \pmod 2$

$\Rightarrow 2/32$

- Order :

Given a number N & x

order is the smallest +ve number r such that $\boxed{x^r \equiv 1 \bmod N}$

e.g $N=17, x=2, r=?$

$2^r \equiv 1 \bmod 17$

$r = 8$

$2^8 = 1 \bmod 17$

Foundation for Advancement of Science & Technology

2) Basic Idea :-

input is a composite number N [N = u.v].

Our goal is to find u and v such that N = u.v

- It uses order finding algo as subroutine. By itself, shor algo is a classical algo based upon simple number theory but it called order finding algorithm to find order which finds order in polynomial time
- It takes a random x, and for that random x it find order r such that ~~x raised to power r is~~

$$x^r \equiv 1 \bmod N \qquad N: \text{input}$$

- Then it checks if our r is even or odd. If r is even then eq is,

$$\left(x^{\frac{r}{2}}\right)^2 - (1)^2 = 0 \bmod N$$

$$\left(x^{\frac{r}{2}} - 1\right)\left(x^{\frac{r}{2}} + 1\right) \equiv 0 \bmod N$$

- The sq. root of x would be either trivial or non-trivial

- By trivial it implies,

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

- In case non trivial,

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

- If $x^{r/2}$ is non-trivial then they will be multiple of u & v. That means this might be

$$\underbrace{\left(x^{r/2} - 1\right)}_{a \times u}\underbrace{\left(x^{r/2} + 1\right)}_{b \times v} \equiv 0 \bmod N$$

Foundation for Advancement of Science & Technology

- In order to retriere u or v from the above we can take gcd of $(x^{r/2}-1)$ with n.
- So, $\gcd(x^{r/2}-1, N) = u$
- Then to find v, $v = \frac{N}{u}$

3) Shor's Algorithm :-

```
while (true) {
    1: choose x randomly where x ∈ {2, N-1}
    2: if ( d = gcd(x, N) ≥ 2) {
            return u = d, v = N/u
       }
    3: find r such that x^r ≡ 1 mod N
    4: if (r is even & d = gcd(x^(r/2) - 1, N) ≥ 2) {
            return u = d, v = N/u
       }
}
```

4) Example:

N = 221.

⇒ 1: x = 5

2: gcd (5, 221) = 1

3: $5^r \bmod 221 \equiv 1$

r = 16

4: 16 is even & d = gcd $(5^8 - 1, 221) = 13$

$u = 13, \quad v = \frac{221}{13} = 17$

Foundation for Advancement of Science & Technology

Quantum Computing
Understanding the order Finding Algo

Problem Definition:-

Given tve integers a and N with $\gcd(a, N) = 1$, our goal is to find the smallest tve integer $r \in \mathbb{Z}_N^*$ such that $a^r \equiv 1 \bmod N$

Example:

$N = 21$, $a = 2$, $r = ?$

$2^r \equiv 1 \bmod 21$

We will try brute force

$r = 1 \Rightarrow 2^1 \equiv 2 \pmod{21}$ X

$r = 2 \Rightarrow 2^2 \equiv 4 \pmod{21}$ X

$r = 3 \Rightarrow 2^3 \equiv 8 \pmod{21}$ X

$r = 4 \Rightarrow 2^4 \equiv 16 \pmod{21}$ X

$r = 5 \Rightarrow 2^5 \equiv 11 \pmod{21}$ X

$r = 6 \Rightarrow 2^6 \equiv 1 \pmod{21}$ ✓

- We can solve order finding algorithm by employing phase estimation algorithm
- In fact order finding is polynomial time reducible to phase estimation algorithm,

order finding $\leq_p$ Phase estimation

- This means that we can take phase estimation algo as a black box we will not change its circuits or anything. we can manipulate its inputs and outputs and by doing this we can realize the order finding algorithm.

Phase Estimation Algorithm:-

Inputs: U (unitary matrix), $|v\rangle$ (Eigenvector of unitary matrix U)

Output: θ (phase) $\in [0,1)$

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

- By calculating θ we can find eigenvalue of unitary matrix U.

- To realize order finding we will prepare a special unitary matrix Lets call it M_α
- Now M_α takes input of $|x\rangle$ where $x \in \mathbb{Z}_N^*$. The output is our input multiplied by α and we also have to calculate our mod.

$$M_\alpha|x\rangle = |\alpha x \pmod N\rangle \quad x \in \mathbb{Z}_N^*$$

- Above is a unitary matrix because it represents a reversible operation we can always find $M_{\alpha^{-1}}$. And $M_{\alpha^{-1}} \cdot M_\alpha = I$
- It is also defined for other values besides the values in the multiplicative group. For these values, input & output remains the same.

Eigenvectors for M: $|\rho_0\rangle, |\rho_1\rangle, |\rho_2\rangle, \ldots, |\rho_{r-1}\rangle$ where $|\rho_j\rangle = \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} \omega_r^{-lj} |\alpha^l\rangle$.

Foundation for Advancement of Science & Technology

Expanded form: $|P_j\rangle = \frac{1}{\sqrt{r}}\left[|1\rangle + \omega_r^{-j}|\alpha\rangle + \omega_r^{-2j}|\alpha^2\rangle + \ldots + \omega_r^{-(r-1)j}|\alpha^{r-1}\rangle\right]$

Eigenvalues for M: $\omega_r^0 = 1, \omega_r^1, \omega_r^2, \ldots, \omega_r^{r-1}$

Verify if eigenvectors & eigenvalues are valid:-

$$M_\alpha |P_j\rangle = \omega_r^j |P_j\rangle$$

LHS:

Applying M_α to $|P_j\rangle$ we would multiply each entry with α

$$\frac{1}{\sqrt{r}}\left[|\alpha\rangle + \omega_r^{-j}|\alpha^2\rangle + \omega_r^{-2j}|\alpha^3\rangle + \ldots + \omega_r^{-(r-1)j}|\alpha^r\rangle\right]$$

Now we take out common ω_r^j

$$\frac{\omega_r^j}{\sqrt{r}}\left[\omega_r^{-j}|\alpha\rangle + \omega_r^{-2j}|\alpha^2\rangle + \omega_r^{-3j}|\alpha^3\rangle + \ldots + \omega_r^{-rj}|\alpha^r\rangle\right]$$

$\therefore \omega_r^r = \omega_r^{r \bmod r} = \omega_r^0 = 1, \quad \alpha^r \equiv 1 \pmod N$

$$\frac{\omega_r^j}{\sqrt{r}}\left[\omega_r^{-j}|\alpha\rangle + \omega_r^{-2j}|\alpha^2\rangle + \omega_r^{-3j}|\alpha^3\rangle + \ldots + |1\rangle\right]$$

Hence, LHS = RHS.

Foundation for Advancement of Science & Technology

Phase Est Algo:-

Input: 1) M_α

2) $|P_1\rangle \sim$ eigenvalue $\omega_r = e^{\frac{2\pi i}{r}}$

Output: $\Theta = \frac{1}{r}$

- We cannot prepare $rho_1(|P_1\rangle)$ before ~~getting~~ knowing r beforehand.
- The solution to this is to give superposition of all the eigenvector as input.

$$\text{Input} = \frac{|P_0\rangle + |P_1\rangle + \ldots + |P_r\rangle}{\sqrt{r}} = |1\rangle$$

- For our output, the output could be Θ of any of the vectors above with equal probability.

$$|P_j\rangle = \omega_r^j$$

$$e^{2\pi i \frac{j}{r}}$$

$$\Theta = \frac{j}{r} \quad j \in [0, r-1]$$

we can retrieve r by performing 2 steps:

1) We will use continuous fraction to write Θ in fractions ~~so~~

2) We will re-run algorithm multiple times. We will get different values of denominator & numerators. In the end we will take LCM of all denominator values and this will give us r with very high probability

$$LCM(r_1, r_2, \ldots) = r$$

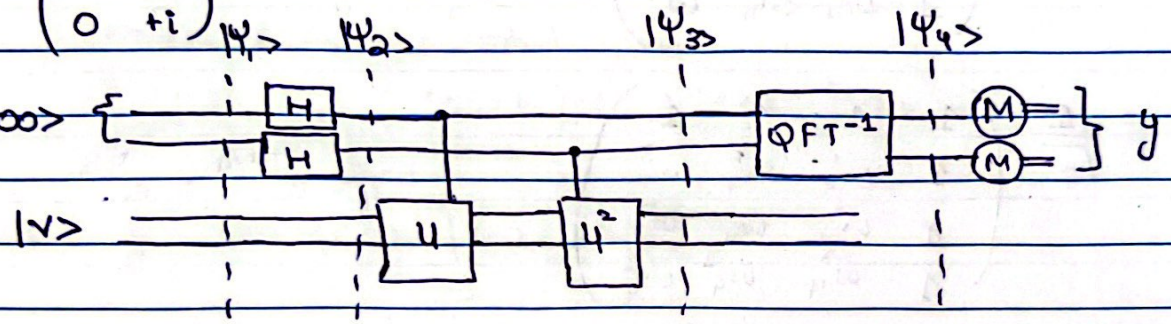
Foundation for Advancement of Science & Technology

Example of Phase Estimation Algorithm:- (2×2 matrix, n=2)

Q. Given a unitary matrix $U = -i|0\rangle\langle 0| + i|1\rangle\langle 1|$ and an eigenvector $|v\rangle = |0\rangle$, estimate 2-bits (size of 1st register (m)) of $\theta \in [0,1)$ such that $U|v\rangle = e^{2\pi i\theta}|v\rangle$

$\Rightarrow$ $e^{2\pi i\theta} = -i$

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



$m = 2$

$\theta = \frac{y}{2^m} = \frac{y}{4}$

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

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

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

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

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

$= \frac{1}{2} \sum_{x=0}^{3} |x\rangle \, (-i)^x |v\rangle$ [Phase kickback concept]

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

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

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

Foundation for Advancement of Science & Technology

on 1st register of $|\psi_3\rangle$.

$$|\psi_4\rangle = QFT^{\dagger}(|\psi_3\rangle)$$

$$\therefore QFT_4^{\dagger} = \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4^1 & \omega_4^2 & \omega_4^3 \\ 1 & \omega_4^2 & \omega_4^4 & \omega_4^6 \\ 1 & \omega_4^3 & \omega_4^6 & \omega_4^9 \end{pmatrix}$$

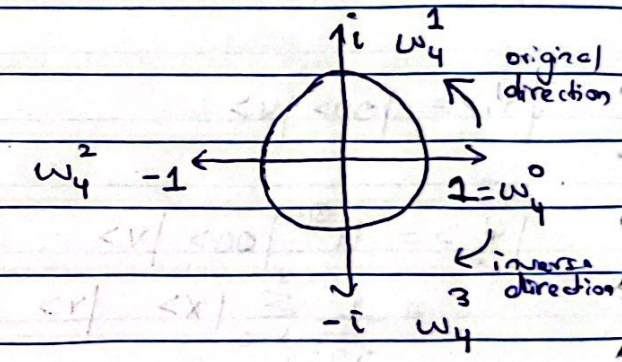
ω represent a modulus function.

$$\omega_4^k = \omega_4^{k \bmod 4}$$

$$= \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4^1 & \omega_4^2 & \omega_4^3 \\ 1 & \omega_4^3 & \omega_4^2 & \omega_4^1 \\ 1 & \omega_4^2 & \omega_4^1 & \omega_4^0 \end{pmatrix}$$

$$\omega_4 = e^{2\pi i/4} = e^{\pi i/2}$$

$$QFT^{\dagger} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & -i & -1 \\ 1 & i & -1 & -i \end{pmatrix}$$



$$|\psi_4\rangle = \frac{1}{2} \times \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & -i & -1 \\ 1 & i & -1 & -i \end{pmatrix} \begin{pmatrix} 1 \\ -i \\ -1 \\ i \end{pmatrix}$$

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

$\boxed{y=3}$

$$\theta = \frac{y}{2^m} = \frac{3}{2^2} = \frac{3}{4}$$

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

Foundation for Advancement of Science & Technology

Q. $U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$, $|v\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\lambda = e^{\frac{i\pi}{4}}$, estimate θ

$\Rightarrow$ We use $|00\rangle$ & $|v\rangle$ as initial inputs

Applying Hadamard on the control qubits:

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

State: $\frac{1}{2}\left[|00\rangle + |01\rangle + |10\rangle + |11\rangle\right]|v\rangle$

Apply Controlled-U, U^2 ... U

$$\frac{1}{2}\left[|00\rangle|v\rangle + |01\rangle U|v\rangle + |10\rangle U^2|v\rangle + |11\rangle U^3|v\rangle\right]$$

Using $U|v\rangle = e^{i\pi/4}|v\rangle$ & $U^2|v\rangle = e^{i\pi/2}|v\rangle$:

$$\frac{1}{2}\left(|00\rangle|v\rangle + |01\rangle e^{i\pi/4}|v\rangle + |10\rangle e^{i\pi/2}|v\rangle + |11\rangle e^{3i\pi/4}|v\rangle\right)$$

Apply inverse QFT

eigenvalue is $e^{i\pi/4}$, so $\lambda = e^{2\pi i\theta}$. Therefore,

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

So,

$$2\pi\theta = \frac{\pi}{4} \Rightarrow \theta = \frac{1}{8}$$

Foundation for Advancement of Science & Technology

Quantum Computing
Properties of Unitary Matrices

A square matrix $U \in \mathbb{C}^{n \times n}$ is unitary if $U^{\dagger}.U = U.U^{\dagger} = I$.
$\Rightarrow U^{\dagger} = U^{-1}$

Example:

Q. $U = \frac{1}{\sqrt{5}} \begin{pmatrix} i & -2i \\ -2i & -i \end{pmatrix}$. Verify if matrix is unitary or not.

$\Rightarrow U^{\dagger} = \frac{1}{\sqrt{5}} \begin{pmatrix} -i & 2i \\ 2i & i \end{pmatrix}$

$$U^{\dagger}U = \frac{1}{5} \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

★ $U^{\dagger}$ is unitary.

Proof:

$(U^{\dagger})^{\dagger}.U^{\dagger} = U^{\dagger}.(U^{\dagger})^{\dagger} = I$

$U.U^{\dagger} = U^{\dagger}U = I$

★ cols of U make orthonormal basis

Proof:

P1: orthonormal

P2: linearly independent

Foundation for Advancement of Science & Technology

P1:

$$\langle c_i | c_j \rangle = \begin{cases} 0 & i \neq j \rightarrow \text{orthogonal} \\ 1 & i = j \rightarrow \text{normalized} \end{cases}$$

$$U^T . U = I$$

$$(c_1\ c_2\ c_3 \cdots c_n)^{\dagger} (c_1\ c_2\ c_3 \cdots c_n) = I$$

$$\begin{pmatrix} c_1^T \\ c_2^{\dagger} \\ c_3^{\dagger} \\ \vdots^{\dagger} \\ c_n^{\dagger} \end{pmatrix} (c_1\ c_2\ c_3 \cdots c_n) = I$$

$$\begin{pmatrix} \langle c_1|c_1\rangle & \langle c_1|c_2\rangle & \langle c_1|c_3\rangle \cdots \langle c_1|c_n\rangle \\ \langle c_2|c_1\rangle & \langle c_2|c_2\rangle & \langle c_2|c_3\rangle \cdots \langle c_2|c_n\rangle \\ \langle c_3|c_1\rangle & \langle c_3|c_2\rangle & \langle c_3|c_3\rangle \cdots \langle c_3|c_n\rangle \\ \vdots & & \\ \langle c_n|c_1\rangle & \langle c_n|c_2\rangle & \langle c_n|c_3\rangle \cdots \langle c_n|c_n\rangle \end{pmatrix}$$

$\therefore \langle c_1|c_1\rangle = \langle c_2|c_2\rangle = \cdots = \langle c_n|c_n\rangle = 1$ (diagonal has all 1's)

$\langle c_1|c_2\rangle = \cdots = 0$

P2:

- Linearly dependent: There exists constants $a_1, a_2, \ldots, a_n$ where atleast one $a_k \neq 0$ such that

$$a_1 \vec{c_1} + a_2 \vec{c_2} + \cdots + a_n \vec{c_n} = 0$$

Foundation for Advancement of Science & Technology

e.g. $\begin{pmatrix} 1 & 2 & 4 \\ 1 & & \\ 1 & 0 & 2 \\ 1 & 1 & 3 \end{pmatrix}$ are columns linearly dependent.

$\Rightarrow a_1\vec{c}_1 + a_2\vec{c}_2 + a_3\vec{c}_3 = \vec{0}$

$2c_1 + c_2 - c_3 = 0$

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

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

Yes, linearly dependent

Proof for P2: Proof By Contradiction

Assume columns of unitary matrix are linearly dependent Hence

$a_1\vec{c}_1 + a_2\vec{c}_2 + \dots + a_n\vec{c}_n = \vec{0}$ — ①

Multiply eq ① with $c_1^\dagger$

$a_1\langle c_1|c_1\rangle + a_2\langle c_1|c_2\rangle + \dots + a_n\langle c_1|c_n\rangle = 0$

$a_1 \cdot 1 + 0 + \dots + 0 = 0$

$a_1 = 0$

Multiply eq ① with $c_2^\dagger$

$a_2 = 0. \Rightarrow \vec{a}_1 = \vec{a}_2 = \dots = \vec{a}_n = 0.$

Hence, assumption is wrong, Thus proving columns are linearly independent

Foundation for Advancement of Science & Technology

★ Rows of U make orthonormal basis.

Proof: Since cols ~~make~~ orthonormal basis ∴ $U^\dagger$ is unitary therefore rows would also hold the same property

★ Unitary matrices preserve inner product of matrices

$$U|\psi_1\rangle = |p_1\rangle$$
$$U|\psi_2\rangle = |p_2\rangle$$
$$\langle\psi_1|\psi_2\rangle = \langle p_1|p_2\rangle$$

Proof:

$$\langle p_1|p_2\rangle = (U|\psi_1\rangle)^\dagger (U|\psi_2\rangle)$$
$$= (\langle\psi_1| U^\dagger)(U|\psi_2\rangle)$$
$$= \langle\psi_1| U^\dagger U|\psi_2\rangle \qquad U^\dagger U = I$$
$$= \langle\psi_1|\psi_2\rangle$$

★ Unitary matrices preserve length (norm) of vectors

$$\| U|\psi_1\rangle \| = \| |\psi_1\rangle \|$$

Proof:

$$\| U|\psi_1\rangle \|$$
$$= \sqrt{(U|\psi_1\rangle)^\dagger \cdot (U|\psi_1\rangle)}$$
$$= \sqrt{\langle\psi_1| U^\dagger U|\psi_1\rangle}$$
$$= \sqrt{\langle\psi_1|\psi_2\rangle} = \| |\psi_1\rangle \|$$
$$= \sqrt{\quad}$$

Foundation for Advancement of Science & Technology

★ Unitary matrices preserve angle between vectors

$$\cos\theta = \frac{\langle \psi_k | \rho \rangle}{\| |\psi\rangle \| \, \| |\rho\rangle \|}$$

Since unitary matrices preserve inner product & p norms, if we apply unitary operator on those vectors the angle b/w vectors will also remain the same.

★ Unitary matrices make a multiplicative group.

A multiplicative group must have the following 4 properties:-

i) It must be closed under multiplication operation
ii) There must exist an identity element for all elements of the group
iii) There must be an inverse for each element of the group
iv) Associativity order of brackets will not matter.

i) if $a, b \in G$ then $a \times b = c \in G$ (must)
ii) $\exists$ an $i \in G$ s.t for each $a \in G$ $a \times i = a$
iii) $\exists$ an inverse for each $a \in G$ $a^{-1} \in G$ $a \times a^{-1} = i$
iv) if $a, b, c \in G$ $(a \times b) \times c = a \times (b \times c)$

Foundation for Advancement of Science & Technology

Proof for properties:

1) Closed under multiplication:

A, B are unitary then $A \times B = C$ must be unitary

$U^\dagger U = I$

$C^\dagger C \stackrel{?}{=} I$

$(AB)^\dagger (AB) \stackrel{?}{=} I$

$B^\dagger A^\dagger A B \stackrel{?}{=} I$

$B^\dagger B \stackrel{?}{=} I$

$I = I$ ✓

2) Identity element for each element of the group

Special matrix

$U \times \square = U \quad \Rightarrow \quad U \times I = U$

$I \in$ unitary matrix

$I^\dagger I = I$

3) Inverse

U is unitary then U^{-1} must be unitary s.t $U \times U^{-1} = I$

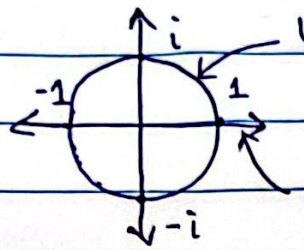
$U^{-1} = U^\dagger$

4) Associativity:

$(A \times B) \times C = A \times (B \times C)$

Foundation for Advancement of Science & Technology

★ Eigenvalues of unitary matrices lie on complex unit circle



$U^\dagger U = I$ (unitary matrices eigenvalues lie on circle)

$H^\dagger = H$ (values of Hermitian matrices lie on real line)

If a matrix is both unitary & hermitian, the what kind of eigenvalues will that matrix have?

⇒ Such a matrix will have values that are an intersection of the ranges of eigenvalues of unitary matrices and eigenvalues of hermitian matrices

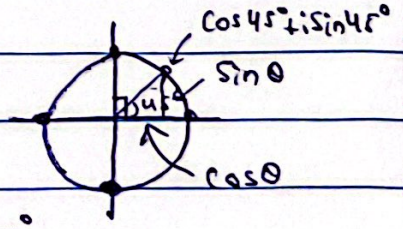
A is both unitary & hermitian. ⇒ Range (U) ∩ Range (H)

$= \{1, -1\}$

• Complex numbers revision:

$$x + iy = r\cos\theta + i\sin\theta$$
$$= re^{i\theta}$$
$$r = |x+iy| = \sqrt{(x+iy)^\dagger (x+iy)}$$
$$= \sqrt{x^2 + y^2}$$
$$\theta = \tan^{-1}\frac{y}{x}$$

Example:



$= \cos 45 + i\sin 45^\circ$

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

$= e^{i\pi/4}$ (Euler constant)

$= \cos 90^\circ + i\sin 90^\circ = i$

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

Foundation for Advancement of Science & Technology

Proof :-

eigenvalue = λ & corresponding eigenvector = $|\psi\rangle$

$U|\psi\rangle = \lambda|\psi\rangle$ (By definition)

unitary matrices preserve norm.

$\| |\psi\rangle \| = \| U|\psi\rangle \|$

$= \| \lambda|\psi\rangle \|$

radius = $|c|$.

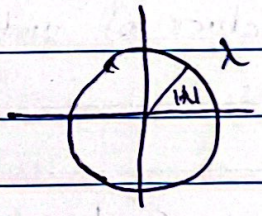
$\| \langle\psi|\psi\rangle \| = \sqrt{(\lambda|\psi\rangle)^\dagger (\lambda|\psi\rangle)}$

$\sqrt{\langle\psi|\psi\rangle} = \sqrt{\langle\psi|\lambda^\dagger \lambda|\psi\rangle}$

$\sqrt{\langle\psi|\psi\rangle} = \sqrt{\lambda^\dagger\lambda}\ \langle\psi|\psi\rangle$

$\sqrt{\langle\psi|\psi\rangle} = \sqrt{\lambda^*\lambda}\ \sqrt{\langle\psi|\psi\rangle}$

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



$|\lambda| = 1$

$\sqrt{\lambda^*.\lambda} = 1$

Foundation for Advancement of Science & Technology

Quantum Computing

Q What is a normal matrix?

⇒ A matrix $N \in C^{n \times n}$ is normal if $N^\dagger N = NN^\dagger$

Example of normal matrices:

① Unitary: $U^\dagger U = UU^\dagger = I$

② Hermitian: $H = H^\dagger = H$

③ Skew-symmetric: $H^\dagger = -H$

Q What is diagonalization?

⇒ Decomposing a matrix into 3 different matrices

$A = P \times D \times P^{-1}$

- Assume matrix A has n different eigenvectors, and are linearly independent = $\{\vec{e_1}, \vec{e_2}, \ldots, \vec{e_n}\}$
- And corresponding eigenvalues are $\lambda_1, \lambda_2, \ldots \lambda_n$

- $P = [\vec{e_1} \quad \vec{e_2} \quad \ldots \quad \vec{e_n}]$

$$D = \begin{bmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{bmatrix}$$

Foundation for Advancement of Science & Technology

Q. What is diagonalization by unitary similarity?

$$N = UDU^{\dagger}$$

N: eigenvectors:
i) linearly independent and
ii) orthonormal

$$U = [\vec{e}_1 \ \vec{e}_2 \ \dots \ \vec{e}_n]$$

$$D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

Q What are the advantages of diagonalization?

- if we have to compute N^{100} we can compute this using diagonalization very quickly (N: matrix)
- Same for e^{iN}, N^{-1}, $\cos(N)$, $\sin(N)$, $N!$

e.g

$$N = UDU^{\dagger}$$

$$N^2 = (UDU^{\dagger})(UDU^{\dagger})$$
$$= UDU^{\dagger}UDU^{\dagger}$$
$$= UD^2U^{\dagger}$$

$$N^{100} = UD^{100}U^{\dagger}$$

$$D = \begin{bmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_n \end{bmatrix} \qquad D^{100} = \begin{bmatrix} d_1^{100} & & & \\ & d_2^{100} & & \\ & & \ddots & \\ & & & d_n^{100} \end{bmatrix}$$

Foundation for Advancement of Science & Technology

- $\sqrt{N} = U \sqrt{D} U^{+}$

Example of Diagonalization by Unitary Similarity:

Hadamard Matrix

Q. $A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ find $\sqrt{A}$ and A^{100}

$\Rightarrow$ $A = UDU^{+}$

$\sqrt{A} = U \sqrt{D} U^{+}$ $\quad A^{100} = UD^{100}U^{+}$

① find eigenvalues of A

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

$$A - \lambda I = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

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

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

$\lambda^2 - 1 = 0 \quad \Rightarrow \lambda = \pm 1$

Foundation for Advancement of Science & Technology

@Eigenvectors:

$\lambda = 1$,

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

$$\left[\begin{array}{cc|c} \frac{1}{\sqrt{2}} - 1 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - 1 & 0 \end{array}\right]$$

$$\left[\begin{array}{cc|c} \frac{1-\sqrt{2}}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1-\sqrt{2}}{\sqrt{2}} & 0 \end{array}\right] \quad \begin{array}{l} R_1 = R_1 \times \sqrt{2} \\ R_2 = R_2 \times \sqrt{2} \end{array}$$

$$\left[\begin{array}{cc|c} 1-\sqrt{2} & 1 & 0 \\ 1 & -1-\sqrt{2} & 0 \end{array}\right] \quad R_1 \leftrightarrow R_2$$

$$\left[\begin{array}{cc|c} 1 & -1-\sqrt{2} & 0 \\ 1-\sqrt{2} & 1 & 0 \end{array}\right] \quad R_2 = R_2 - (1-\sqrt{2})R_1$$

$$\left[\begin{array}{cc|c} 1 & -1-\sqrt{2} & 0 \\ 0 & 0 & 0 \end{array}\right]$$

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

$x_2 = s = 1$

$$x_1 + (-1-\sqrt{2})x_2 = 0$$

$$x_1 = 1 + \sqrt{2}$$

$$\lambda_1 = 1, \quad \vec{x} = \begin{bmatrix} 1+\sqrt{2} \\ 1 \end{bmatrix}$$

Foundation for Advancement of Science & Technology

$\lambda = -1$,

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

$$\left[\begin{array}{cc|c} \frac{1}{\sqrt{2}}+1 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}}+1 & 0 \end{array}\right] = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

$$\left[\begin{array}{cc|c} \frac{1+\sqrt{2}}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{-1+\sqrt{2}}{\sqrt{2}} & 0 \end{array}\right] \quad R_1 = R_1 \times \sqrt{2}, \quad R_2 = R_2 \times \sqrt{2}$$

$$\left[\begin{array}{cc|c} 1+\sqrt{2} & 1 & 0 \\ 1 & -1+\sqrt{2} & 0 \end{array}\right] \quad R_1 \leftrightarrow R_2$$

$$\left[\begin{array}{cc|c} 1 & -1+\sqrt{2} & 0 \\ 1+\sqrt{2} & 1 & 0 \end{array}\right] \quad R_2 = R_2 - (1+\sqrt{2})R_1$$

$$\left[\begin{array}{cc|c} 1 & -1+\sqrt{2} & 0 \\ 0 & 0 & 0 \end{array}\right] \qquad 1-(1+\sqrt{2})(-1+\sqrt{2}) = 0$$

$y_2 = s = 1$ $\qquad y_1 + (-1+\sqrt{2})y_2 = 0$

$y_1 = 1 - \sqrt{2}$

$\lambda = -1$, $\vec{y} = \begin{bmatrix} 1-\sqrt{2} \\ 1 \end{bmatrix}$

Foundation for Advancement of Science & Technology

(2) (3) Verify that vectors are orthogonal to each other & normalized.

$$\langle \vec{x} | \vec{y} \rangle = (1+\sqrt{2})(1-\sqrt{2}) + 1$$
$$= 1 - 2 + 1 = 0 \quad \checkmark$$

Not normalized. Hence we need to normalize vectors.

$$\|\vec{x}\| = \sqrt{(1+\sqrt{2})(1+\sqrt{2}) + (1)(1)}$$
$$= \sqrt{1+2+2\sqrt{2}+1}$$
$$= \sqrt{4+2\sqrt{2}}$$

$$\vec{x} = \frac{1}{\sqrt{4+2\sqrt{2}}} \begin{bmatrix} 1+\sqrt{2} \\ 1 \end{bmatrix}$$

$$\|\vec{y}\| = \sqrt{(1-\sqrt{2})(1-\sqrt{2}) + (1)(1)}$$
$$= \sqrt{1+2-2\sqrt{2}+1}$$
$$= \sqrt{4-2\sqrt{2}}$$

$$\vec{y} = \frac{1}{\sqrt{4-2\sqrt{2}}} \begin{bmatrix} 1-\sqrt{2} \\ 1 \end{bmatrix}$$

Foundation for Advancement of Science & Technology

(4) Now we can write matrix in diagonalization form

$$A = UDU^{\dagger}$$

$$A = \begin{pmatrix} \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}} \\ \frac{1}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4+2\sqrt{2}}} \\ \frac{1-\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}} \end{pmatrix}$$

$$\sqrt{A} = U\sqrt{D}U^{\dagger}$$

$$\sqrt{D} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$. Rest would remain same

$$\sqrt{A} = \frac{1}{4}\begin{pmatrix} 2+\sqrt{2}+i(-\sqrt{2}+2) & \sqrt{2}-i\sqrt{2} \\ \sqrt{2}-i\sqrt{2} & (2-\sqrt{2})+i(\sqrt{2}+2) \end{pmatrix}$$

$$A^{100} = UD^{100}U^{\dagger}$$

$$D^{100} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^{100} = I$$