Shor Algorithm

1) Background
2) Basic idea
3) Shor algo
4) Shor example

Modulus :-

$$20 \equiv 2 \pmod 3$$

(20 is same as 2 it is because if we divide 20 from 3 our remainder is 2.)

Similarly :-

$$2 \equiv 20 \pmod 3$$

Similarly :-

$$20 \bmod 3 \equiv 2$$

Divisibility :-

$$a \equiv 0 \bmod N$$

$$N \mid a$$

$$32 \equiv 0 \bmod 2$$

Order

Given N, x

order is a the smallest +ve number r s.t

$$\boxed{x^r \equiv 1 \bmod N}$$

Example :-

$N = 17$, $x = 2$

$r = ?$

$2^r \equiv 1 \mod 17$

Key idea:-

input N (It is composite of two prime u and v)

Goal u, v s.t N = u x v

$x^r \equiv 1 \mod N$

then check if our r is even or odd

if (r == even)

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

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

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

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

$a \times v \quad b \times v$

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

$v = N/u$

proper steps:-

while (true) {

1: choose $x \in (2, N-1)$

2: if $(d = \gcd(x, N) \geq 2)$ {

return $u = d$, $v = N/u$ }

3: find r, s.t $x^r = 1 \mod N$

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

return $u = d$, $v = N/u$. }

Example :-

$N = 221$

1: $x = 5$

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

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

$r = \cancel{96}\, 16$

4) as r = even && $d = \gcd(5^{16/2} - 1, \cancel{N}\ 221) \geq 2$

$u = d = 13$

$v = 221/13 = 17$

return u, v

Order Finding Algorithm

Problem Definition :-

Given positive integers α and N with ~~gcd~~ ~~α~~ $\gcd(\alpha, N) = 1$, Find the smallest positive integer $r \in Z_N^*$ s.t

$\alpha^{r} \equiv 1 \pmod N$

Example:-

$N = 21$, $\alpha = 2$, $r = ?$

$\alpha^{r} \equiv 1 \bmod \cancel{21}\, N$	$2^6 = 64 \equiv 1 \bmod 21$ ✓
$2^{r} \equiv 1 \bmod 21$	So $r = 6$
$r=1$ × $2^1 = 2 \bmod 21$ ×	
× $2^2 = 4 \bmod \bmod 21$	
× $2^3 = 8 \bmod 21$	
× $2^4 = 16 \bmod 21$	
× $2^5 = 32 = \cancel{\bmod}\ 11 \bmod 21$	

Order finding $\angle_p$ Phase estimation

Phase Estimation

Input ① U
② $|v\rangle$

Output $\theta \in [0,1)$
such that $U|v\rangle = e^{2\pi i \theta}|v\rangle$

To realise order finding the basic idea is we will prepare a special unitary matrix let e call this M_α, it eigen value has order r in it.

$$M_\alpha |x\rangle = |\alpha x (\bmod N)\rangle \qquad x \in Z_N^*$$

$$M \cdot M_{\alpha^{-1}} = I$$

Eigen vectors $|P_0\rangle\ |P_1\rangle\ |P_2\rangle \ldots\ |P_{r-1}\rangle$ $\qquad |P_j\rangle = \frac{1}{\sqrt{r}} \sum_{i=0}^{r-1} \omega_r^{-ij} |\alpha^i\rangle$

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

Eigen value

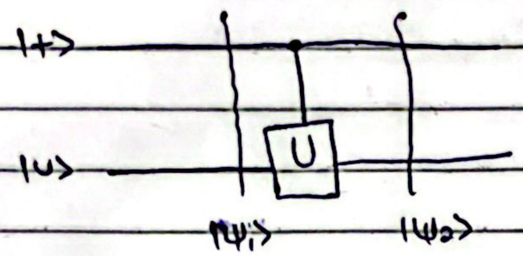
$$\omega_r^0 = 1,\ \omega_r,\ \omega_r^2, \ldots, \omega_r^{r-1}$$

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

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

Phase Kickback

Consider this circuit :-



let say $|v\rangle$ is an eigenvector of U so if we apply U gate to state v we get

$$U|v\rangle = e^{i\theta}|v\rangle$$

since all the eigen value can be represented as e to the i θ.

So now

$$|\psi_1\rangle = |+\rangle|u\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle + |1\rangle|u\rangle\right)$$

$$|\psi_2\rangle = \frac{1}{2}\left(CU|0\rangle|v\rangle + CU|1\rangle|v\rangle\right)$$

nothing happens to the first superposition since the control is zero, but in second superposition state has the gate applied

$$\frac{1}{\sqrt{2}}\left(|0\rangle|v\rangle + e^{i\theta}|1\rangle|v\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)|v\rangle$$

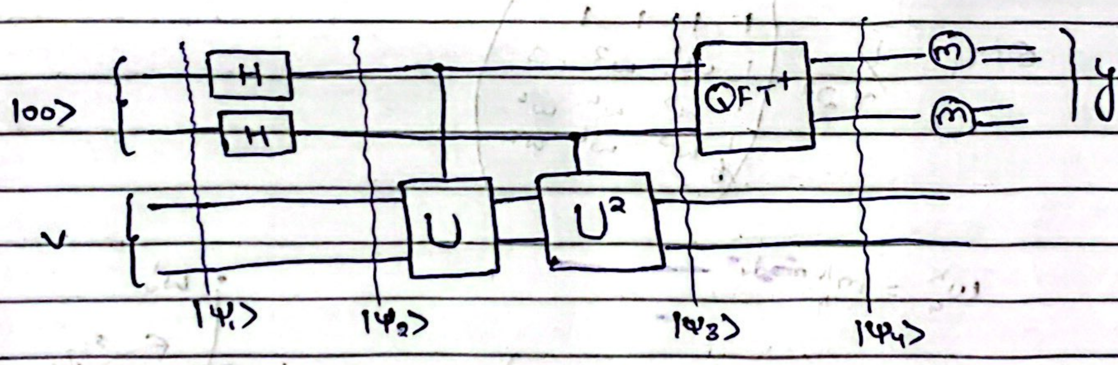
If we have a state $|v\rangle$ that is an eigen vector of gate U, by apply a Controlled-U gate with $|v\rangle$ as the target we can kick the phase onto the control qubit.

Phase Estimation

Ex Given a unitary matrix $U = -i|0\rangle\langle 0| + i|1\rangle\langle 1|$ and an eigen vector $|v\rangle = |0\rangle$ estimate $\underline{2\text{-bits}}$ of $\theta \in [0,1)$ s.t. $U|v\rangle = e^{2\pi i\theta}|v\rangle$

$\searrow$ eigen value $= -i$

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



$\theta = y/2^m$

$\theta = y/4$

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

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

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

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

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

Phase kickback

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

Scanned with CamScanner

$$|\psi_3\rangle = \frac{1}{2}\left[(i)^0|0\rangle + (-i)^1|1\rangle + (-i)^2|2\rangle + (-i)^3|3\rangle \right]$$

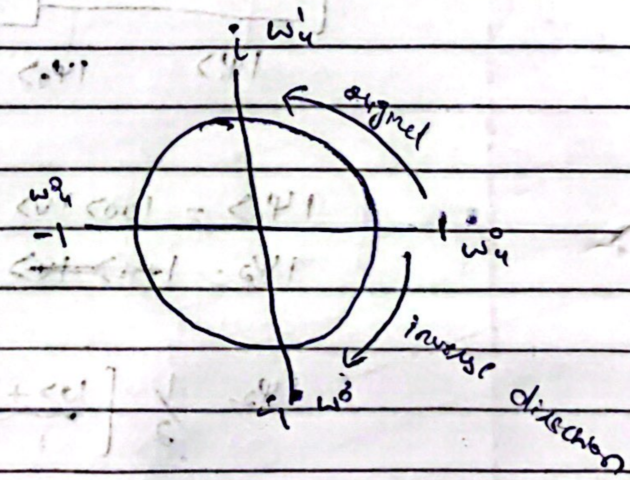
$$= \frac{1}{2}\left[|0\rangle - i|1\rangle - |2\rangle + i|3\rangle \right]$$

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

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

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

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



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

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

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

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

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

Quantum Computing

Simon's Algorithm

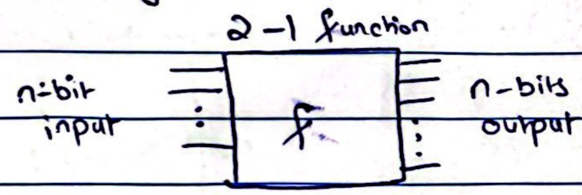
Problem Definition:-

Given a 2-1 function

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

$f(x) = f(x \oplus S)$ for $S \in \{0,1\}$

Our goal is to find S



For exactly 2 input the functions produces a same output

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

It produce same output for input x and for input x xor with a secret message S and our goal is to fin the S.

Example:-

n = 3 (implies the function will take 3-bit input and give 3-bit output)

S = 101

$n=3$ $S=101$ size of domain $=2^n$

domain x (All binary string of length 3)	Range $f(x)$
000	111
001	000
010	110
011	010
100	000
101	111
110	010
111	110

if we give random output such as 000 is 111 then same output will appear on 101.

if we take XOR of

$$\begin{array}{r} 001 \; x \\ \oplus\; 101 \; S \\ \hline 100 \end{array}$$

The function is 2-1 it implies that for exactly half of the inputs the function will produce unique outputs. 2^{n-1}.

half input
ie 2^{n-1} produce unique output

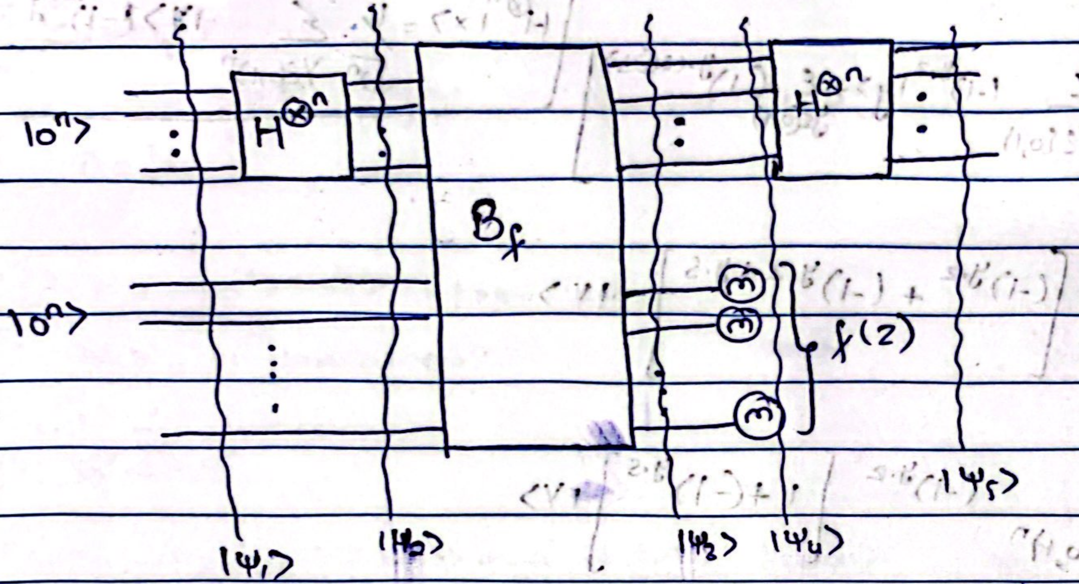
In order to find two inputs with the same output
In the worst case $2^{n-1}+1$

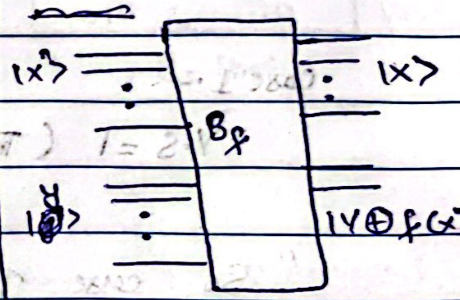
$$2^{n-1}+1 \longrightarrow O(2^n)$$

In Quantum Algo

$O(n) \rightarrow$ linear running time

Circuit of Simon's Algo





So in our case $|y\rangle = |0\rangle$

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

we ge $|f(x)\rangle$

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

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

$$= \frac{1}{2^{n/2}} \sum_{x\in\{0,1\}} |x\rangle|0^n\rangle$$

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

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

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

Foundation for Advancement of Science & Technology

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

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

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

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

Case 1:-

$y\cdot s = 1$ (The probabity that $y\cdot s = 1$ is 0 because thare amplitude is equal 0)

"So case 1 can never exist"

Case 2:-

$y\cdot s = 0$

2^{n-1} goal n-1 linearly independent value of Y.

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

Example:

Same diagram as on previous page.

$n = 4$

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

$S = 1001$

$$|\psi_1\rangle = |0^4\rangle |0^4\rangle = |0000\rangle |0000\rangle$$

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

$$= \frac{1}{2^4} \sum_{x \in \{0,1\}^n} |x\rangle |0000\rangle$$

$$= \frac{|0000\rangle + |0001\rangle + |0010\rangle + \dots + |1111\rangle}{4} |0000\rangle$$

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

$$= \frac{1}{4} \Big[|0000\rangle |1111\rangle + |0001\rangle |0001\rangle + |0010\rangle |1110\rangle + \dots + |1111\rangle |1010\rangle \Big]$$

$$|\psi_4\rangle = \frac{|z\rangle + |z \oplus s\rangle}{\sqrt{2}} |f(z)\rangle$$ so for example we measure $1010 \doteq f(z)$

$$|\psi_4\rangle = \frac{|0110\rangle + |1111\rangle}{\sqrt{2}} |1010\rangle$$

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

$$|\psi_5\rangle = |0000\rangle - |0010\rangle - |0100\rangle + |0110\rangle + |1001\rangle - |1011\rangle - |1101\rangle + |1111\rangle$$

Properties of Eigen Values & Eigenvector

① eigen vector cannot be $\vec{0}$ (Null vector)

② Two eigen vector can have same eigen value

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad x_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ \lambda_2 = 2$$

$$x_2 \begin{bmatrix} 0 \\ 21 \end{bmatrix}; \ \lambda_2 = 2$$

③ $A_{n \times n}$ can have at most n linearly independent vector.

④ If $A\vec{x} = \lambda\vec{x}$ then $A\vec{y} = \lambda\vec{y}$ where $\vec{y} = 9\vec{x}$

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

$$A 2\vec{x} \quad \lambda \underbrace{2\vec{x}}_{y}$$

$$A\vec{y} = \lambda\vec{y}$$

⑤ Trace rule

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \text{sum of eigen value}$$

$$= 1 + 5 + 9 = 15$$

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

⑦ Diagonal rule

$$\begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix} \quad \begin{array}{l} \lambda_1 = a_{11} \\ \lambda_2 = a_{22} \\ \lambda_3 = a_{33} \end{array}$$

$$x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad x_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

⑧ Triangular matrix :-

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

$\lambda_1 = a_{11}$ $\quad x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

$\lambda_2 = a_{22}$ $\quad$ ~~$x_2 =$~~

$\lambda_3 = a_{33}$ $\quad$ ...

⑨ eigenvalue of A = eigenvalue of A^T

⑩ If λ is eigen value of A then λ^k is eigen value of A^k

$A = \lambda_1 = 5 \quad \lambda_2 = 3 \qquad A^{-1} = \lambda_1 = 1/5 \quad \lambda_2 = 1/3$

Foundation for Advancement of Science & Technology

(11) For matrix A $\lambda_i = 0$ then $|A| = 0$ A is regular.

(12) All row has some sum $\&$ then $\lambda = 8$ $X = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$

Example :-

2 eigenvector and 3 eigen value of following matrix.

(a) $\begin{pmatrix} 5 & 0 & 13 \\ 0 & 19 & 24 \\ 0 & 0 & 14 \end{pmatrix}$

$\lambda_1 = 5$ $\quad x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

$\lambda_2 = 19$ $\quad x_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

$\lambda_3 = 14$

(b) $\begin{pmatrix} 2 & 8 & 0 \\ 5 & 5 & 0 \\ 1 & 2 & 7 \end{pmatrix}$

$\lambda_1 = 7$ $\quad x_1 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ $\quad \lambda_3 = \text{Trace} - (\lambda_1 + \lambda_3)$

$= 14 - (17)$

$\lambda_2 = 10$ $\quad x_2 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ $\quad = -3$

Foundation for Advancement of Science & Technology

Ex. Find determinant of the following matrix using eigenvalue

$$A = \begin{pmatrix} 1 & 5 & 3 \\ 0 & 5 & 0 \\ 9 & 0 & 7 \end{pmatrix}$$

$$A^T = \begin{pmatrix} 1 & 0 & 9 \\ 5 & 5 & 0 \\ 3 & 0 & 7 \end{pmatrix}$$

$\lambda_1 = 5$

$\lambda_2 = 10$

$\lambda_3 = \text{Trace} - (\lambda_1 + \lambda_2)$

$= 13 - 15$

$= -2$

$\det = 5 \times 10 \times -2 = -100$

Example :-

Find eigenvalue and eigenvector for matrix

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

Sol:-

Step 1:-

~~$\lambda_1 = 3$ and $\lambda_2 = 4$~~

$|A - \lambda I| = 0$

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

Foundation for Advancement of Science & Technology

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

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

$$=(3-\lambda)(4-\lambda) = 0$$

$$\lambda=3 \quad , \quad \lambda=4$$

Step 2:- find eigenvector for $\lambda_1 = 3$

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

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

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

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

$$\left(\begin{array}{cc|c} 2 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right) \quad R_1 \leftrightarrow R_2$$

$$x_1 = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

Properties of Eigen Values & Eigenvector

① eigen vector cannot be $\vec{0}$ (Null vector)

② Two eigen vector can have same eigen value

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad x_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \lambda_2 = 2$$

$$x_2 \begin{bmatrix} 0 \\ 21 \end{bmatrix}; \quad \lambda_2 = 2$$

③ $A_{n \times n}$ can have at most n linearly independent vector.

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

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

$$A a\vec{x} \quad \lambda \underbrace{a\vec{x}}_{y}$$

$$A\vec{y} = \lambda\vec{y}$$

⑤ Trace rule

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \text{Sum of eigen value}$$

$$= 1 + 5 + 9 = 15$$

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

⑦ Digonal rule

$$\begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{pmatrix} \qquad \begin{aligned} \lambda_1 &= a_{11} \\ \lambda_2 &= a_{22} \\ \lambda_3 &= a_{33} \end{aligned}$$

$x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \quad x_2 \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \quad x_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

⑧ Triangular matrix :-

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

$\lambda_1 = a_{11}$ $\quad x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

$\lambda_2 = a_{22}$ $\quad \cancel{x_2}$

$\lambda_3 = a_{33}$

⑨ eigenvalue of A = eigenvalue of A^T

⑩ If λ is eigen value of A then λ^k is eigen value of A^k

$A = \lambda_1 = 5 \quad \lambda_2 = 3 \qquad A^{-1} = \lambda_1 = 1/5 \quad \lambda_2 = 1/3$

$A^2 \quad \lambda_1 = 25 \quad \lambda_2 = 9$

(11) For matrix A $\lambda_i = 0$ then $|A| = 0$ A is regular.

(12) All row has same sum ℓ then $\lambda = \ell$ $X = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$

Example :-

2 eigenvector and 3 eigen value of following matrix.

(a) $\begin{pmatrix} 5 & 0 & 13 \\ 0 & 19 & 24 \\ 0 & 0 & 14 \end{pmatrix}$

$\lambda_1 = 5$ $x_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$

$\lambda_2 = 19$ $x_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

$\lambda_3 = 14$

(b) $\begin{pmatrix} 2 & 8 & 0 \\ 5 & 5 & 0 \\ 1 & 2 & 7 \end{pmatrix}$

$\lambda_1 = 7$ $x_1 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ $\lambda_3 = \text{Trace} - (\lambda_1 + \lambda_3)$

$= 14 - (17)$

$\lambda_2 = 10$ $x_2 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ $= -3$

Ex. Find determinant of the following matrix using eigenvalue

$$A = \begin{pmatrix} 1 & 5 & 3 \\ 0 & 5 & 0 \\ 9 & 0 & 7 \end{pmatrix}$$

$$A^T = \begin{pmatrix} 1 & 0 & 9 \\ 5 & 5 & 0 \\ 3 & 0 & 7 \end{pmatrix}$$

$\lambda_1 = 5$

$\lambda_2 = 10$

$\lambda_3 = \text{Trace} - (\lambda_1 + \lambda_2)$

$= 13 - 15$

$= -2$

$\det = 5 \times 10 \times -2 = -100$

Example :-

Find eigenvalue and eigenvector for matrix

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

Sol:-

Step 1:-

$\cancel{\lambda_1 = 3 \text{ and } \lambda_2} = 4$

$|A - \lambda I| = 0$

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

Foundation for Advancement of Science & Technology

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

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

$$(3-\lambda)(4-\lambda) = 0$$

$$\lambda=3 \quad , \quad \lambda=4$$

Step 2:- find eigenvector for $\lambda_1 = 3$

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

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

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

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

$$\left(\begin{array}{cc|c} 2 & 1 & 0 \\ 0 & 0 & 0 \end{array}\right) \quad R_1 \leftrightarrow R_2$$

$$x_1 = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$$

Properties of Unitary Matrices

A matrix $U \in \mathbb{C}^{n\times n}$ (complex entries) is unitary if
$U^+ \cdot U = U \cdot U^+ = I$

$\Rightarrow U^+ = U^{-1}$

Example:-

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

verify if U is unitary

Sol:

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

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

Properties:-

① U^+ is a unitary

Proof

U^+ is unitary

$(U^+)^+ U^+ = U^+ \cdot (U^+)^+ = I$

$U \cdot U^+ = U^+ \cdot U = I$

② Cols of U make orthonormal basis

To Part of proof

$\underline{P_1}$ orthonormal

$\underline{P_2}$ linearly independent

$\ldots\ldots + 0 =$

Part - I

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

$$U^{+} \cdot U = I$$

$$= \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix}^{+} \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_n \end{pmatrix}$$

$$= \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{pmatrix} \begin{pmatrix} c_1 c_2 c_3 \cdots c_n \end{pmatrix} = I$$

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

$$= \underbrace{\langle c_1|c_1\rangle = \langle c_2|c_2\rangle = \cdots = \langle c_n|c_n\rangle = 1}_{\text{The diagonel of } I \text{ matrix is } 1}$$

so it is ~~orthono~~ normelized

$\langle c_1 | c_2 \rangle = 0$

P_2 linearly independent :-

Def linear dependent :-

$\exists$ Constant $a_1, a_2, \dots, a_n$ where at least one $a_x \neq 0$ s.t

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

Example :-

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

Col are linearly dependent?

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

$$2\vec{c}_1 + \vec{c}_2 - \vec{c}_3 = \vec{0}$$

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

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

so they are linearly dependent

Now we have to prove the col of unitary matrix are linearly independent

Proof by contradiction

Assume col of U are dep hence

$$a_1\vec{c}_1 + a_2\vec{c}_2 + \dots + a_n\vec{c}_n = 0 \quad \text{--- (1)}$$

mul (1) with $c_1^\dagger$.

$$a\langle\vec{c}_1|\vec{c}_1\rangle + a_2\langle\vec{c}_1|\vec{c}_2\rangle + \dots a_n\langle\vec{c}_1|\vec{c}_n\rangle$$

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

$a_1 \cdot 1 = 0$

$a_1 = 0$

Mul eq 1 with C_2^{+}

:

$a_2 = 0$

$\vec{a}_1 = \vec{a}_2 = \cdots = \vec{a}_n = 0$

Hence my assumption was wrong

Hence all col of Unitary matrix are IND

③ Row of U make an orthonormal basis

④ Unitary matrices pressewe inner product.

$U|\psi_1\rangle = |\phi_1\rangle$

$U|\psi_2\rangle = |\phi_2\rangle$

$\langle \psi_1 | \psi_2 \rangle = \langle \phi_1 | \phi_2 \rangle$

<u>Proof</u>

$\langle \phi_1 | \phi_2 \rangle = (U|\psi\rangle)^{+} (U|\psi_2\rangle)$

$= \langle \psi_1 | U^{+} U | \psi_2 \rangle$

$= \langle \psi_1 | \psi_2 \rangle$

⑤ Unitary matrices pressewe norm of ~~the~~ vectors.

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

Proof

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

$$= \sqrt{(U|\psi_1\rangle)^{+}\cdot(U|\psi_2\rangle)}$$

$$= \sqrt{\langle\psi_1|U^{+}U|\psi_1\rangle}$$

$$= \sqrt{\langle\psi_1|\psi_2\rangle}$$

$$= ||\,|\psi_1\rangle||$$

⑥ Unitary matrix preserve angle b/w vectors.

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

⑦ Unitary matrices make a multiplicative group.

$G, \times$

i) Closed under $\times$

if $a, b \in G$ then $a \times b = c \in G$ (must)

ii) $\exists$ an $i \in G$ such for each $a \in G$ $a \times i = a$

iii) There must exist an inverse for each $a \in G$.

$a^{-1} \in G$

$a \times a^{-1} = i$

iv) Associativity

if $a, b, c \in G$

$((a \times b) \times c) = (b \times c) \times a$

1) Closed

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

$U^{+} \cdot U = I$

$C^{+} \times C = I$

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

$B^{+} \underbrace{A^{+} A}_{I} B = I$

I

$I = I$

②

$U \times \boxed{I} = U$

$I \in$ unitary matrix

$I^{+} I = I$

③ inverse

U is unitary

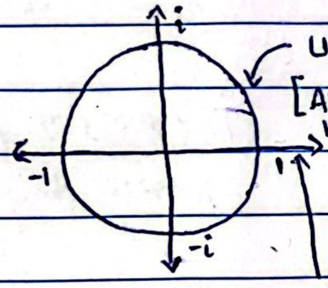
U^{-1} must be unitary

$U \cdot U^{-1} = I$

④

Eigen value of a unitary Matrix lie on Unit Circle

(8) It implies that we have a circle and the circle is unit circle because its radius is equal to 1 and the circle has of 2 axis going through it so we have imaginary axis. and we have real axis



$UU^{\dagger} = I$

[All the eigen value of unitary matrix on this circle]

[whereas all the eigen values of harmisen matrix lie on real line]

$H^{\dagger} = H$

Let say A matrix which is both unitary and Harmition. So It eigen values will be. intersection of range of eigen value of unitary matrices. and range of eigen value of Harmiton matrix.

$$\text{Range}(U) \cap \text{Range}(H)$$

As you can see the circle and real line are intersecting at two points therefore our answer will be either 1 or -1

$x + iy = r\cos\theta + i r\sin\theta$

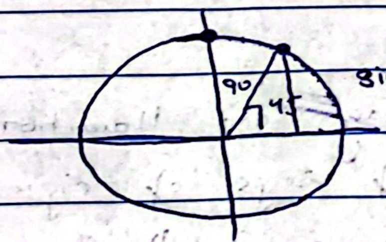
$= re^{i\theta}$ (euler constant)

$r = |x + iy| = \sqrt{(x+iy)^* (x+iy)}$

$= \sqrt{x^2 + y^2}$

$\theta = \tan^{-1} \frac{y}{x}$

Example:-



~~cos~~ $= 1 \cos 45 + i(1) \sin 45$

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

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

$= \cos 90 + i \sin 90$

$= i$

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

eigenvalue $= \lambda$

eigenvector $= |\psi\rangle$

By definition:-

$$U|\psi\rangle = \lambda|\psi\rangle$$

unitary matrix preserve norm

$$\| \, |\psi\rangle \, \| = \| U|\psi\rangle \|$$
$$= \| \lambda|\psi\rangle \|$$

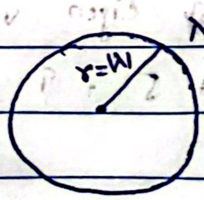
$$\sqrt{\langle\psi|\psi\rangle} = \sqrt{(\lambda|\psi\rangle)^* (\lambda|\psi\rangle)}$$

$$\sqrt{\langle\psi|\psi\rangle} = \sqrt{\langle\psi|\lambda^* \lambda|\psi\rangle}$$

$$= \sqrt{\lambda^* \lambda \langle\psi|\psi\rangle}$$

$$\sqrt{\langle\psi|\psi\rangle} = \sqrt{\lambda^* \lambda} \sqrt{\langle\psi|\psi\rangle}$$
$$\sqrt{\langle\psi|\psi\rangle} = |\lambda| \sqrt{\langle\psi|\psi\rangle}$$

$$|\lambda| = 1$$



9. Normal matrix is always diagonalizable by a unitary similarity.

Q What is a normal matrix?

A matrix $N \in C^{n \times n}$ is normal if $N^{+}N = NN^{+}$

Examples

- Unitary matrices
  - $U^{+}U = UU^{+} = I$
- Hermition matrices:-
  - $H^{+} = H$
- Skew symmetric
  - $H^{+} = -H$

Q What is diagonalization:-

If the matrix is decomposeble into three different matrices then matrix $A = PDP^{-1}$ is diagonalizable

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

eigenvector of A are linearly independent

$$\{\vec{e}, \vec{e}_2, \ldots, \vec{e}_n\}$$

corresponding eigenvalue are

$$\lambda_1, \lambda_2 \ldots \lambda_n$$

$$P = \begin{bmatrix} \vec{e} & \vec{e}_2 & \cdots & \vec{e}_n \end{bmatrix} \quad D = \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots & \\ & & & \lambda_n \end{bmatrix}$$

Q. what is diagonalization by unitary similarity.

$$N = UDU^+$$

N's eigen vector
- linearly independent.
- orthonormal.

$$U = \begin{bmatrix} \vec{e}_1 & \vec{e}_2 & \cdots & \vec{e}_n \end{bmatrix}$$

$$D = \begin{bmatrix} \lambda_1 & & \\ & \lambda_2 & \\ & & \ddots \lambda_n \end{bmatrix}$$

Q advantages of diagonalization?

$$N = UDU^+$$

$$N^2 = (UDU^+)(UDU^+)$$
$$= UDU^+UDU^+$$
$$= UD^2U^+$$

$$N^{100} = UD^{100}U^+$$

$$D^{100} = \begin{bmatrix} \alpha_1^{100} & 0 & 0 & 0 \\ 0 & \alpha_2^{100} & 0 & 0 \\ 0 & 0 & \ddots & \\ 0 & 0 & & \alpha_n^{100} \end{bmatrix}$$

Example :

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

find $\sqrt{A}$ & A^{100}

$\sqrt{A} = \cancel{UD} \; U D^{1/2} U^{+}$

$A^{100} = U D^{100} U^{+}$

Sol:-

① Find eigen values

$\{A - \lambda I\}$

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

$\cancel{\lambda = 1/\sqrt{2} \quad \lambda = -1/\sqrt{2}}$

$$= \begin{bmatrix} 1/\sqrt{2} - \lambda & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \quad \lambda_1 = 1/\sqrt{2}$$

$\lambda_2 = -1/\sqrt{2}$

② Determinment

$$|A - \lambda I| = \left(\frac{1}{\sqrt{2}} - \lambda\right)\left(\frac{-1}{\sqrt{2}} - \lambda\right) - \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}$$

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

$= \lambda^2 - 1 = 0 \qquad \lambda = \pm 1$

Eigen vector

$\lambda = 1 \qquad (A - \lambda I)\vec{x} = \vec{0}$

$$\left[\begin{array}{cc|c} \frac{1}{\sqrt{2}} - 1 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} - 1 & 0 \end{array}\right] \quad \begin{array}{l} R_1 = R_1 \times \sqrt{2} \\ R_2 = R_2 \times \sqrt{2} \end{array}$$

$$\left[\begin{array}{cc|c} 1 - \sqrt{2} & 1 & 0 \\ 1 & -1 - \sqrt{2} & 0 \end{array}\right] \quad R_1 \leftrightarrow R_2$$

$$\left[\begin{array}{cc|c} 1 & -1 - \sqrt{2} & 0 \\ 1 - \sqrt{2} & \cancel{1 - \sqrt{2}}\ 1 & 0 \end{array}\right] \quad R_2 = R_2 - (1 - \sqrt{2})R_1$$

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

$x_2 = s = 1$

$x_1 + (-1 - \sqrt{2})x_2 = 0$

$x_1 = 1 + \sqrt{2}$

$$\lambda = 1 \cdot \quad \vec{x} = \begin{bmatrix} 1 + \sqrt{2} \\ 1 \end{bmatrix}$$

Eigen vector for $\lambda = -1$

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

$$\left[\begin{array}{cc|c} 1/\sqrt{2} + 1 & 1/\sqrt{2} & 0 \\ 1/\sqrt{2} & -1/\sqrt{2} + 1 & 0 \end{array}\right]$$

$R_1 = \sqrt{2} R_1 \qquad R_2 = \sqrt{2} R_2$

$$\left[\begin{array}{cc|c} 1+\sqrt{2} & 1 & 0 \\ 1 & -1+\sqrt{2} & 0 \end{array}\right]$$

$R_1 \leftrightarrow R_2$

$$\left[\begin{array}{cc|c} 1 & -1+\sqrt{2} & 0 \\ 1+\sqrt{2} & 1 & 0 \end{array}\right]$$

$R_2 = R_2 - (1+\sqrt{2}) R_1$

$$\left[\begin{array}{cc|c} 1 & -1+\sqrt{2} & 0 \\ 0 & 0 & 0 \end{array}\right]$$

$x_2 = s = 1$

$\lambda = -1 \quad \vec{x} = \begin{bmatrix} 1-\sqrt{2} \\ 1 \end{bmatrix}$

$x_1 + (-1+\sqrt{2}) x_2 = 0$

$x_1 = 1 - \sqrt{2}$

~~Convert~~ Confirm whether they vector are orthogonal and normalised.

$$\langle \vec{x} | \vec{y} \rangle = (1+\sqrt{2})(1-\sqrt{2}) + 1$$
$$= 1 - 2 + 1 = 0$$
orthogonal

Convert into normalised

$$\|\vec{x}\| = \sqrt{(1+\sqrt{2})^* (1+\sqrt{2}) + 1 \cdot 1}$$
$$= \sqrt{1 + 2 + 2\sqrt{2} + 1}$$
$$= \sqrt{4 + 2\sqrt{2}}$$

$$\vec{x}_1 = \frac{1}{4+2\sqrt{2}} \begin{bmatrix} 1+\sqrt{2} \\ 1 \end{bmatrix}$$

$$\|x_2\| = \sqrt{(1-\sqrt{2})(1-\sqrt{2}) + (1 \cdot 1)}$$
$$= \sqrt{1 - \sqrt{2} + 2\sqrt{2} + 1}$$
$$= \sqrt{4 - 2\sqrt{2}}$$

$$x_2 = \frac{1}{\sqrt{4-2\sqrt{2}}} \begin{bmatrix} 1-\sqrt{2} \\ 1 \end{bmatrix}$$

now they are normalised

$A = UDU^{+}$

$$A^{1/2} = \begin{pmatrix} \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}} \\ \frac{1}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} \frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4+2\sqrt{2}}} \\ \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}} \end{pmatrix}$$

$$\sqrt{A} = \frac{1}{4} \begin{pmatrix} 2+\sqrt{2}+i(\sqrt{2}+2) & \sqrt{2}-i\sqrt{2} \\ \sqrt{2}-i\sqrt{2} & (2-\sqrt{2})+i(\sqrt{2}+2) \end{pmatrix}$$

for A^{100}

$$A^{100} = \begin{pmatrix} & \\ & // & \\ & \end{pmatrix} \begin{pmatrix} 1^{100} & 0 \\ 0 & -1^{100} \end{pmatrix}$$

$$A^{100} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

if we power Hademard with any even we get identity.

Scanned with CamScanner