Abdullah Awan
21L-7713

QUANTUM COMPUTING

Assignmen 01

Q#01

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

Eigen values: $|A - I\lambda| = 0$

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

determinet:

$$= (3-\lambda)[(2-\lambda)(1-\lambda)] - 1[(1-\lambda)+1] + (-1)[(2-\lambda)]$$
$$= (3-\lambda)[2-2\lambda-\lambda+\lambda^2] + [\lambda-2] + [\lambda-2]$$
$$= (3-\lambda)[2-2\lambda-\lambda+\lambda^2] + \lambda-2+\lambda-2$$
$$= 6-6\lambda-3\lambda+3\lambda^2-2\lambda+2\lambda^2+\lambda^2-\lambda^3+2\lambda-4$$
$$= -\lambda^3+6\lambda^2-9\lambda+2=0$$

Eigen values:

$$\lambda_1 = 2+\sqrt{3}, \quad \lambda_2 = 2, \quad \lambda_3 = 2-\sqrt{3}$$

Eigenvectors:

$$(A - \lambda I)x = 0$$

$$\lambda_1 = 2 + \sqrt{3}$$

$$\left[\begin{array}{ccc|c} 3-(2+\sqrt{3}) & 1 & -1 & 0 \\ 1 & 2-(2+\sqrt{3}) & 1 & 0 \\ -1 & 0 & 1-2-\sqrt{3} & 0 \end{array}\right]$$

$$\left[\begin{array}{ccc|c} 1-\sqrt{3} & 1 & -1 & 0 \\ 1 & -\sqrt{3} & 1 & 0 \\ -1 & 0 & -1-\sqrt{3} & 0 \end{array}\right]$$

Reduced row echlon form:

$R_1 / 1-\sqrt{3}$:

$$\left[\begin{array}{ccc} 1 & 1/1-\sqrt{3} & (1+\sqrt{3})/2 \\ 1 & -\sqrt{3} & 1 \\ -1 & 0 & -\sqrt{3}-1 \end{array}\right]$$

$R_2 - R_1$:

$$\left[\begin{array}{ccc} 1 & 1/1-\sqrt{3} & (1+\sqrt{3})/2 \\ 0 & -(-1+\sqrt{3})/2 & -(-1+\sqrt{3})/2 \\ -1 & 0 & -\sqrt{3}-1 \end{array}\right]$$

$R_3 + R_1$:

$$\left[\begin{array}{ccc} 1 & 1/1-\sqrt{3} & (1+\sqrt{3})/2 \\ 0 & -(-1+\sqrt{3})/2 & -(-1+\sqrt{3})/2 \\ 0 & \frac{1}{1-\sqrt{3}} & \frac{-1+\sqrt{3}}{2} \end{array}\right]$$

$R_2 \times \frac{-2}{-1+\sqrt{3}}$:

$$\begin{bmatrix} 1 & 1/1-\sqrt{3} & (1+\sqrt{3})/2 \\ 0 & 1 & 1 \\ 0 & 1/1-\sqrt{3} & -1+\sqrt{3}/2 \end{bmatrix}$$

$R_1 - \frac{R_2}{1-\sqrt{3}}$:

$$\begin{bmatrix} 1 & 0 & 1+\sqrt{3} \\ 0 & 1 & 1 \\ 0 & \frac{1}{1-\sqrt{3}} & \frac{-1+\sqrt{3}}{2} \end{bmatrix}$$

$R_3 - \frac{R_2}{1-\sqrt{3}}$:

$$\begin{bmatrix} 1 & 0 & 1+\sqrt{3} \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

Since:

$$\left[\begin{array}{ccc|c} 1 & 0 & 1+\sqrt{3} & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

So:

$$x_1 + (1+\sqrt{3})x_3 = 0$$
$$x_2 + x_3 = 0$$

let $x_3 = t$

$$x_1 = t(-\sqrt{3}-1), \quad x_2 = -t$$

$$x_1 = \begin{bmatrix} -\sqrt{3}-1 \\ -1 \\ 1 \end{bmatrix} \qquad \lambda_1 = 2+\sqrt{3}$$

$\lambda_2 = 2$

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

$R_2 - R_1$:

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

$R_3 + R_1$: $\begin{bmatrix} 1 & 1 & -1 \\ 0 & -1 & 2 \\ 0 & 1 & -2 \end{bmatrix}$

$R_2(-1)$: $\begin{bmatrix} 1 & 1 & -1 \\ 0 & 1 & -2 \\ 0 & 1 & -2 \end{bmatrix}$

$R_3 - R_2$: $\begin{bmatrix} 1 & 1 & -1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix}$

$R_1 - R_2$: $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 0 \end{bmatrix}$

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

$x_1 + x_3 = 0$

$x_2 - 2x_3 = 0$

$x_3 = t$

$x_1 = -t \;,\; x_2 = 2t \;,\; x_3 = t$

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

$\lambda_3 = 2 - \sqrt{3}$

$$\begin{bmatrix} 3-2+\sqrt{3} & 1 & -1 \\ 1 & \sqrt{3} & 1 \\ -1 & 0 & -1+\sqrt{3} \end{bmatrix}$$

$R_1 : \frac{R_1}{1+\sqrt{3}}$

$$\begin{bmatrix} 1 & -1+\sqrt{3}/2 & -(-1+\sqrt{3})/2 \\ 1 & \sqrt{3} & 1 \\ -1 & 0 & -1+\sqrt{3} \end{bmatrix}$$

$R_2 - R_1 :$

$$\begin{bmatrix} 1 & -1+\sqrt{3}/2 & -(-1+\sqrt{3})/2 \\ 0 & 1+\sqrt{3}/2 & 1+\sqrt{3}/2 \\ (-1) & 0 & -1+\sqrt{3} \end{bmatrix}$$

$R_3+R_1:\begin{bmatrix} 1 & -1+\sqrt{3}/2 & -(-1+\sqrt{3})/2 \\ 0 & 1+\sqrt{3}/2 & 1+\sqrt{3}/2 \\ 0 & -1+\sqrt{3}/2 & -1+\sqrt{3}/2 \end{bmatrix}$

$\frac{R_2 \times 2}{1+\sqrt{3}}:\begin{bmatrix} 1 & -1+\sqrt{3}/2 & -(-1+\sqrt{3})/2 \\ 0 & 1 & 1 \\ 0 & -1+\sqrt{3}/2 & -1+\sqrt{3}/2 \end{bmatrix}$

$R_1-R_2\left(\frac{-1+\sqrt{3}}{2}\right):\begin{bmatrix} 1 & 0 & 1-\sqrt{3} \\ 0 & 1 & 1 \\ 0 & \frac{-1+\sqrt{3}}{2} & \frac{-1+\sqrt{3}}{2} \end{bmatrix}$

$R_3-R_2\left(\frac{-1+\sqrt{3}}{2}\right):\begin{bmatrix} 1 & 0 & 1-\sqrt{3} \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$

$x_1+(1-\sqrt{3})x_3=0 \;,\; x_2+x_3=0 \;,\; x_3=t$

$x_1=t(-1+\sqrt{3}) \;,\; x_2=-t \;,\; x_3=t$

$x_3=\begin{bmatrix} -1+\sqrt{3} \\ -1 \\ 1 \end{bmatrix}$, $\lambda_3=2-\sqrt{3}$

$\lambda_1=2+\sqrt{3}$, $x_1=\begin{bmatrix} -\sqrt{3}-1 \\ -1 \\ 1 \end{bmatrix}$ $x_2=\begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix}$ $x_3=\begin{bmatrix} -1+\sqrt{3} \\ -1 \\ 1 \end{bmatrix}$

$\lambda_2=2$,

$\lambda_3=2-\sqrt{3}$,

Q#02(a)

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

Using diagonal rule:

$$\lambda_1 = 7 \;, \quad \overrightarrow{x_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\lambda_2 = -1 \;, \quad \overrightarrow{x_2} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Q#02(b)

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 3 \\ 0 & 0 & 5 \end{pmatrix}$$

$\lambda_1 = 1 \;, \quad \lambda_2 = 2 \;, \quad \lambda_3 = x$

det : $= (1)([2+5]+[3\times 0])+2([0\times 0]+[2\times 0])$

$= 1\,(10+0) = 10$

Using determinant rule:

$10 = \lambda_1 \times \lambda_2 \times \lambda_3$

$10 = 1 \times 2 \times x$

$10 = 2x$

$x = 10/2$

$\boxed{x = 5}$

$\vec{x_1} : \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ $\vec{x_2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

$\vec{x_3} : \begin{bmatrix} 1-\lambda & 0 & 2 \\ 0 & 2-\lambda & 3 \\ 0 & 0 & 5-\lambda \end{bmatrix} \Rightarrow \begin{bmatrix} -4 & 0 & 2 \\ 0 & -3 & 3 \\ 0 & 0 & 0 \end{bmatrix}$

$$\left[\begin{array}{ccc|c} -4 & 0 & 2 & 0 \\ 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

$-\frac{1}{4} \times R_1$: $\left[\begin{array}{ccc|c} 1 & 0 & -1/2 & 0 \\ 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$

$-\frac{1}{3} \times R_2$: $\left[\begin{array}{ccc|c} 1 & 0 & -1/2 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$

$x_1 - \frac{x_3}{2} = 0$, $x_2 - x_3 = 0$, $x_3 = t$

$x_1 = \frac{t}{2}$, $x_2 = t$, $x_3 = t$

$\vec{x_3} = \begin{bmatrix} 1/2 \\ 1 \\ 1 \end{bmatrix}$

$\lambda_1 = 1$
$\lambda_2 = 2$
$\lambda_3 = 5$

$\rightarrow \quad \vec{x_1} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \vec{x_2} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \quad \vec{x_3} = \begin{bmatrix} 1/2 \\ 1 \\ 1 \end{bmatrix}$

Q#02(c)

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

$\lambda_1 = 1, \quad \vec{x_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \lambda_2 = x$

using determinant rule:

$(1 \times 4) - (0 \times 3) = 1 \times x$

$\boxed{x = 4}$

$\lambda_2 = 4$

$$\vec{x_2} = \left(\begin{array}{cc|c} -3 & 3 & 0 \\ 0 & 1 & 0 \end{array}\right)$$

$$R_1 \times \frac{-1}{3} : \left(\begin{array}{cc|c} 1 & -1 & 0 \\ 0 & 1 & 0 \end{array}\right)$$

$x_1 - x_2 = 0$

$x_2 = t$

$x_1 = t, \quad x_2 = t$

$$\vec{x_2} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$\lambda_1 = 1$, $\vec{x_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\vec{x_2} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

$\lambda_2 = 4$,

Q#03:

$N = 437$

1) $x = 3$

2) $d = GCD\ (3, 437)$

3) $x^r = 1 \bmod 437$

$3^r = 1 \bmod 437$

$\vdots$

$r = 198$

4) 198 is even

$d = GCD\ (3^{99} - 1, 437) = 23$

$23 > 2 \rightarrow$ True

$u = 23$, $v = \frac{437}{23} = 19$

Prime factors of 437 = 23 and 19

Q#04:

Proof:

Based on unitary matrices preserving norm of vectors

Given eigen value λ & eigen vector $|\psi\rangle$:

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

$\Rightarrow$ $|\psi\rangle$'s norm before unitary transformation must be equal to $|\psi\rangle$'s norm after unitary transformation

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

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

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

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

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

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

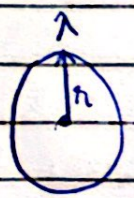
$$\sqrt{\langle\psi|\psi\rangle} = |\lambda| \cdot \sqrt{\langle\psi|\psi\rangle}$$

- $|\lambda|$ tells how far eigenvalues is from unit circle's center

L·H·S = R·H·S if $|\lambda| = 1$

$\overline{|\lambda^* \lambda} = 1$

So, above proves that eigenvalues lie on complex unit circle with $r = 1$



$r = |\lambda| = 1$

Q#05(a)

$p = 13$, $q = 7$

$n = p \times q = 13 \times 7 = 91$

For Totient function:

$\phi(n) = (13^1 - 13^0) \times (7^1 - 7^0)$

$= 12 \times 6 = 72$

Public Key:

$1 \bmod 5 = 2$

$5 \bmod 2 = 1$

$\therefore$ $e = 5$ (prime number) for factorization

$e \times d = 1 \pmod{\phi(n)}$

Private Key:

$d = 29$ (Extended Eucledian)

Q#05(b)

$\therefore x = 3$

Encryption at Sender $= y = x^e \pmod n$

$= 3^5 \bmod 91$

$= 243 \bmod 91$

$\boxed{y = 61}$

Q#05(c)

Decryption at receiver:

$= y^d \pmod n \quad \therefore d = 29$

$= 61^{29} \pmod{91}$

$= 3$ (By modular Exponentiation Method)