Hilbert spaces and unitary matrices

Question 1. Define

$$H_2 = \mathbb{C}^2 = \{\ \alpha|0\rangle + \beta|1\rangle \ \mid\ \alpha, \beta \in \mathbb{C}\ \}$$

The inner product in H_2 is defined by

$$\langle\ \alpha_1|0\rangle + \beta_1|1\rangle \mid \alpha_2|0\rangle + \beta_2|1\rangle\ \rangle \quad = \quad \alpha_1^\dagger \alpha_2 + \beta_1^\dagger \beta_2$$

for all $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$. Show that the inner product satisfies the following four properties:

1. $\langle \varphi \mid \varphi \rangle \geq 0$
2. $\langle \varphi \mid \varphi \rangle = 0$ if and only if $|\varphi\rangle = 0$.
3. $\langle \varphi \mid \psi \rangle = \langle \psi \mid \varphi \rangle^\dagger$.
4. $\langle \varphi \mid \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \varphi \mid \psi_1 \rangle + \lambda_2 \langle \varphi \mid \psi_2 \rangle$

for any $|\varphi\rangle, |\psi\rangle, |\psi_1\rangle, |\psi_2\rangle \in H_2$ and for any $\lambda_1, \lambda_2 \in \mathbb{C}$.

Question 2. Prove that all the matrices in the catalog of matrices (given earlier) are unitary.

Question 3. Show that if U is unitary, then $U^\dagger$ is unitary.

Question 4. Show that the product of two unitary matrices is unitary.

Question 5. For any complex $N \times N$ matrix U, we can uniquely write $U = R + iQ$, where R and Q have real entries. Show that if U is unitary, then so is the $2N \times 2N$ matrix U' given in block form by

$$U' \quad = \quad \begin{pmatrix} R & Q \\ -Q & R \end{pmatrix}$$

Thus, by doubling the dimension, we can remove the need for complex-number entries. Show the result of applying this construction to the Pauli matrix Y.

Question 6. Show that the four Pauli matrices X, Y, Z, I form an orthonormal basis for the space of 2×2 matrices. Thus, we can regard the space of 2×2 matrices as a 4-dimensional complex Hilbert space.

Question 1. Define

$$H_2 = \mathbb{C}^2 = \{\ \alpha|0\rangle + \beta|1\rangle \ \mid\ \alpha, \beta \in \mathbb{C}\ \}$$

The inner product in H_2 is defined by

$$\langle\ \alpha_1|0\rangle + \beta_1|1\rangle \mid \alpha_2|0\rangle + \beta_2|1\rangle\ \rangle \ = \ \alpha_1^\dagger \alpha_2 + \beta_1^\dagger \beta_2$$

for all $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$. Show that the inner product satisfies the following four properties:

1. $\langle \varphi \mid \varphi \rangle \geq 0$

Since $|\varphi\rangle \in H_2$, its inner product is $\langle \varphi | \varphi \rangle = \langle \alpha_1|0\rangle + \beta_1|1\rangle \mid \alpha_1|0\rangle + \beta_1|1\rangle \rangle$

$$\langle \varphi | \varphi \rangle = \langle \alpha_1|0\rangle \mid \alpha_1|0\rangle + \alpha_1|0\rangle \mid \beta_1|1\rangle + \beta_1|1\rangle \mid \alpha_1|0\rangle + \beta_1|1\rangle \mid \beta_1|1\rangle \rangle$$

$$= \alpha_1^* \alpha_1 \underbrace{\langle 0|0\rangle}_{1} + \alpha_1^* \beta_1 \underbrace{\langle 0|1\rangle}_{0} + \beta_1^* \alpha_1 \underbrace{\langle 1|0\rangle}_{0} + \beta_1^* \beta_1 \underbrace{\langle 1|1\rangle}_{1}$$

$$= \alpha_1^* \alpha_1 + \beta_1^* \beta_1$$

$$= |\alpha_1|^2 + |\beta_1|^2$$

Since $|\alpha_1|^2$ and $|\beta_1|^2$ are always non-negative, the sum of them are non-negative, $|\alpha_1|^2 + |\beta_1|^2 \geq 0$

$\therefore \langle \varphi | \varphi \rangle = |\alpha_1|^2 + |\beta_1|^2 \geq 0$

2. $\langle \varphi \mid \varphi \rangle = 0$ if and only if $|\varphi\rangle = 0$.

Prove $\langle \varphi | \varphi \rangle = 0$ if $|\varphi\rangle = 0$

$|\varphi\rangle = 0$. So it is a zero vector (all components of vector are 0)

$\langle \varphi | \varphi \rangle = \sum \varphi_i^* \cdot \varphi_i = 0 \cdot 0 = 0$

Prove that $|\varphi\rangle = 0$ if $\langle \varphi | \varphi \rangle = 0$

As we proved in (a), $\langle \varphi | \varphi \rangle = |\alpha_1|^2 + |\beta_1|^2$, $|\alpha_1|^2 + |\beta_1|^2 = 0$

$\therefore \alpha_1 = \beta_1 = 0$

$\therefore |\varphi\rangle = \alpha_1|0\rangle + \beta_1|1\rangle = 0$

$\therefore \langle \varphi | \varphi \rangle = 0$ if and only if $|\varphi\rangle = 0$

3. $\langle \varphi \mid \psi \rangle = \langle \psi \mid \varphi \rangle^{\dagger}$.

$$< \varphi | \psi > = < \begin{pmatrix} \varphi_0 \\ \vdots \\ \varphi_{k-1} \end{pmatrix} | \begin{pmatrix} \psi_0 \\ \vdots \\ \psi_{k-1} \end{pmatrix} = \sum_i \varphi_i^* \cdot \psi_i$$

$$< \psi | \varphi > = \sum_i \psi_i^* \cdot \varphi_i \, ,$$

$$< \psi | \varphi >^{\dagger} = \left(\sum_i \psi_i^* \cdot \varphi_i \right)^* = \sum_i (\psi_i^*)^* \cdot \varphi_i^*$$

$$= \sum_i \psi_i \cdot \varphi_i^*$$

$$\therefore < \varphi | \psi > = \sum_i \varphi_i^* \cdot \psi_i = \sum_i \psi_i \cdot \varphi_i^* = < \psi | \varphi >^{\dagger}$$

4. $\langle \varphi \mid \lambda_1 \psi_1 + \lambda_2 \psi_2 \rangle = \lambda_1 \langle \varphi \mid \psi_1 \rangle + \lambda_2 \langle \varphi \mid \psi_2 \rangle$

$$< \varphi | \lambda_1 \psi_1 + \lambda_2 \psi_2 >$$

$$= \sum_i (\varphi_i)^* \cdot (\lambda_1 \psi_1 + \lambda_2 \psi_2)_i$$

$$= \sum_i (\varphi_i)^* \cdot (\lambda_1 \psi_1)_i + (\varphi_i)^* \cdot (\lambda_2 \psi_2)_i$$

$$= \sum_i (\varphi_i)^* \cdot (\lambda_1 \psi_1)_i + \sum_i (\varphi_i)^* \cdot (\lambda_2 \psi_2)_i \, .$$

Since λ_1 and λ_2 are complex number

$$= \lambda_1 \sum_i (\varphi_i)^* \cdot (\psi_1)_i + \lambda_2 \sum_i (\varphi_i)^* \cdot (\psi_2)_i$$

$$= \lambda_1 < \varphi | \psi_1 > + \lambda_2 < \varphi | \psi_2 >$$

$\therefore$ Proved.

Question 2. Prove that all the matrices in the catalog of matrices (given earlier) are unitary.

A linear operation U is unitary iff $UU^\dagger = U^\dagger U = I$.

① $X = \begin{pmatrix}0&1\\1&0\end{pmatrix}$, $X^\dagger = \begin{pmatrix}0&1\\1&0\end{pmatrix}$ $\quad X^\dagger X = XX^\dagger = \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix} = I$

∴ X is unitary

② $Y = \begin{pmatrix}0&-i\\i&0\end{pmatrix}$ $\quad Y^T = \begin{pmatrix}0&i\\-i&0\end{pmatrix}$ $\quad Y^\dagger Y = YY^\dagger = \begin{pmatrix}0&-i\\i&0\end{pmatrix}\begin{pmatrix}0&-i\\i&0\end{pmatrix} = \begin{pmatrix}0\cdot0+(-i)\cdot i & 0(-i)+(-i)\cdot0\\ i\cdot0+0\cdot i & i\cdot(-i)+0\cdot0\end{pmatrix}$

$Y^\dagger = \begin{pmatrix}0&-i\\i&0\end{pmatrix}$ $\qquad = \begin{pmatrix}1&0\\0&1\end{pmatrix} = I$

∴ Y is unitary.

③ $Z = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$ $\quad Z^\dagger = \begin{pmatrix}1&0\\0&-1\end{pmatrix}$ $\quad Z^\dagger Z = ZZ^\dagger = \begin{pmatrix}1&0\\0&-1\end{pmatrix}\begin{pmatrix}1&0\\0&-1\end{pmatrix} = \begin{pmatrix}1\cdot1+0\cdot0 & 1\cdot0+0\cdot(-1)\\ 0\cdot1+(-1)\cdot0 & 0\cdot0+(-1)(-1)\end{pmatrix}$

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

∴ Z is unitary

④ $I = \begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\quad I^\dagger = \begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\quad I^\dagger I = II^\dagger = \begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix} = I$

∴ I is unitary

⑤ $H = \frac{1}{\sqrt2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ $\quad H^\dagger = \frac{1}{\sqrt2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ $\quad H^\dagger H = HH^\dagger = \frac{1}{\sqrt2}\cdot\frac{1}{\sqrt2}\begin{pmatrix}1\cdot1+1\cdot1 & 1\cdot1+1\cdot(-1)\\ 1\cdot1+(-1)\cdot1 & 1\cdot1+(-1)(-1)\end{pmatrix} = \frac12\begin{pmatrix}2&0\\0&2\end{pmatrix}$

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

∴ H is unitary.

⑥ $R_x(\theta) = \begin{pmatrix}\cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2})\\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix}$, $\quad R_x(\theta)^\dagger = \begin{pmatrix}\cos(\frac{\theta}{2}) & i\sin(\frac{\theta}{2})\\ i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{pmatrix}$

$R_x(\theta)R_x(\theta)^\dagger = \begin{pmatrix}\cos(\frac{\theta}{2})\cdot\cos(\frac{\theta}{2}) + (-i\sin(\frac{\theta}{2}))\cdot i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\cdot(i\sin(\frac{\theta}{2})) + (-i\sin(\frac{\theta}{2}))\cdot\cos(\frac{\theta}{2})\\ (-i\sin(\frac{\theta}{2}))\cdot\cos(\frac{\theta}{2}) + \cos(\frac{\theta}{2})\cdot i\sin(\frac{\theta}{2}) & (-i\sin(\frac{\theta}{2}))\cdot i\sin(\frac{\theta}{2}) + \cos(\frac{\theta}{2})\cos(\frac{\theta}{2})\end{pmatrix}$

$= \begin{pmatrix}(\cos(\frac{\theta}{2}))^2 + (\sin(\frac{\theta}{2}))^2(-i)(i) & 0\\ 0 & (-i)(i)(\sin(\frac{\theta}{2}))^2 + (\cos(\frac{\theta}{2}))^2\end{pmatrix}$

$= \begin{pmatrix}(\cos(\frac{\theta}{2}))^2 + (\sin(\frac{\theta}{2}))^2 & 0\\ 0 & (\sin(\frac{\theta}{2}))^2+(\cos(\frac{\theta}{2}))^2\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix} = I$

$$R_x(\theta)^\dagger R_x(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2})\cdot\cos(\frac{\theta}{2}) + (-i\sin(\frac{\theta}{2}))\cdot i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\cdot(-i\sin(\frac{\theta}{2})) + i\sin(\frac{\theta}{2})\cdot\cos(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2})\cdot\cos(\frac{\theta}{2}) + \cos(\frac{\theta}{2})\cdot(-i\sin(\frac{\theta}{2})) & i\sin(\frac{\theta}{2})(-i\sin(\frac{\theta}{2})) + \cos(\frac{\theta}{2})\cdot\cos(\frac{\theta}{2}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \quad \therefore R_x(\theta) \text{ is unitary.}$$

⑦ $R_y(\theta) = \begin{pmatrix} \cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$ $\quad R_y(\theta)^\dagger = \begin{pmatrix} \cos(\frac{\theta}{2}) & \sin(\frac{\theta}{2}) \\ -\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$

$$R_y(\theta)\, R_y(\theta)^\dagger = \begin{pmatrix} (\cos(\frac{\theta}{2}))^2 + (-\sin(\frac{\theta}{2}))^2 & \cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) - \sin(\frac{\theta}{2})\cos(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2})\cos(\frac{\theta}{2}) + \cos(\frac{\theta}{2})(-\sin(\frac{\theta}{2})) & (\sin(\frac{\theta}{2}))^2 + (\cos(\frac{\theta}{2}))^2 \end{pmatrix}$$

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

$$R_y(\theta)^\dagger R_y(\theta) = \begin{pmatrix} (\cos(\frac{\theta}{2}))^2 + (\sin(\frac{\theta}{2}))^2 & \cos(\frac{\theta}{2})(-\sin(\frac{\theta}{2})) + \sin(\frac{\theta}{2})\cos(\frac{\theta}{2}) \\ -\sin(\frac{\theta}{2})\cos(\frac{\theta}{2}) + \cos(\frac{\theta}{2})\sin(\frac{\theta}{2}) & (-\sin(\frac{\theta}{2}))^2 + \cos(\frac{\theta}{2}))^2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \qquad \therefore R_y(\theta) \text{ is unitary.}$$

⑧ $R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$ $\quad R_z(\theta)^\dagger = \begin{pmatrix} e^{i\frac{\theta}{2}} & 0 \\ 0 & e^{-i\frac{\theta}{2}} \end{pmatrix}$

$$R_z(\theta)\, R_z(\theta)^\dagger = \begin{pmatrix} (e^{-i\frac{\theta}{2}})\cdot e^{i\frac{\theta}{2}} + 0\cdot 0 & 0\cdot e^{-i\frac{\theta}{2}} + 0\cdot e^{-i\frac{\theta}{2}} \\ 0\cdot e^{i\frac{\theta}{2}} + e^{i\frac{\theta}{2}}\cdot 0 & 0\cdot 0 + e^{i\frac{\theta}{2}}\cdot e^{-i\frac{\theta}{2}} \end{pmatrix} = \begin{pmatrix} e^0 & 0 \\ 0 & e^0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

$$R_z(\theta)^\dagger R_z(\theta) = \begin{pmatrix} e^{i\frac{\theta}{2}}\cdot e^{-i\frac{\theta}{2}} + 0\cdot 0 & 0 \\ 0 & 0\cdot 0 + e^{-i\frac{\theta}{2}}\cdot e^{i\frac{\theta}{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \quad \therefore R_z(\theta) \text{ is unitar}$$

⑨ $R_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$ $\quad R_\varphi^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}$ $\quad R_\varphi R_\varphi^\dagger = \begin{pmatrix} 1\cdot 1 + 0\cdot 0 & 1\cdot 0 + 0\cdot e^{-i\varphi} \\ 0\cdot 1 + e^{i\varphi}\cdot 0 & 0\cdot 0 + e^{i\varphi}\cdot e^{-i\varphi} \end{pmatrix}$

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

$$R_\varphi^\dagger R_\varphi = \begin{pmatrix} 1\cdot 1 + 0\cdot 0 & 1\cdot 0 + 0\cdot e^{i\varphi} \\ 0\cdot 1 + e^{-i\varphi}\cdot 0 & 0\cdot 0 + e^{-i\varphi}\cdot e^{i\varphi} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \quad \therefore R_\varphi \text{ is unitary}$$

⑩ $S=\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. $S^{\dagger}=\begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$ $SS^{\dagger}=\begin{pmatrix} 1\cdot1+0\cdot0 & 1\cdot0+0\cdot(-i) \\ 0\cdot1+i\cdot0 & 0\cdot0+i\cdot(-i) \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I$

$S^{\dagger}S=\begin{pmatrix} 1\cdot1+0\cdot0 & 1\cdot0+0\cdot i \\ 0\cdot1+(-i)\cdot0 & 0\cdot0+(-i)\cdot i \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I$ $\therefore$ S is unitary.

⑪ $T=\begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$ $T^{\dagger}=\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix}$ $TT^{\dagger}=\begin{pmatrix} 1\cdot1+0\cdot0 & 1\cdot0+0\cdot e^{-i\frac{\pi}{4}} \\ 0\cdot1+e^{i\frac{\pi}{4}}\cdot0 & 0\cdot0+e^{i\frac{\pi}{4}}\cdot e^{-i\frac{\pi}{4}} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & e^{0} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I$

$T^{\dagger}T=\begin{pmatrix} 1\cdot1+0\cdot0 & 1\cdot0+0\cdot e^{i\frac{\pi}{4}} \\ 0\cdot1+e^{-i\frac{\pi}{4}}\cdot0 & 0\cdot0+e^{-i\frac{\pi}{4}\cdot i\frac{\pi}{4}} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=I$ $\therefore$ T is unitary

Question 3. Show that if U is unitary, then $U^\dagger$ is unitary.

By definition, the linear operation M is unitary iff

$$MM^\dagger = M^\dagger M = I$$

If U is unitary, $UU^\dagger = U^\dagger U = I$.

The conjugate transpose of $U^\dagger$ is $(U^\dagger)^\dagger = U$.

$\therefore U^\dagger (U^\dagger)^\dagger = U^\dagger U$, $(U^\dagger)^\dagger U^\dagger = UU^\dagger$

$\because UU^\dagger = U^\dagger U = I$ $\therefore U^\dagger (U^\dagger)^\dagger = (U^\dagger)^\dagger U^\dagger = I$ $\therefore U^\dagger$ is unitary

$\therefore$ If U is unitary, then $U^\dagger$ is unitary

Question 4. Show that the product of two unitary matrices is unitary.

U and V are two unitary matrices

$\therefore UU^\dagger = U^\dagger U = I$, $VV^\dagger = V^\dagger V = I$

To show $U \cdot V$ is unitary, we need to prove that

$$(U \cdot V) \cdot (U \cdot V)^\dagger = (U \cdot V)^\dagger \cdot (U \cdot V) = I$$

$(U \cdot V) \cdot (U \cdot V)^\dagger = (U \cdot V) \cdot (V^\dagger \cdot U^\dagger)$ since $(UV)^\dagger = V^\dagger U^\dagger$

$= U \cdot (V \cdot V^\dagger) \cdot U^\dagger = U \cdot I \cdot U^\dagger = U \cdot U^\dagger = I$

$(U \cdot V)^\dagger (U \cdot V) = (V^\dagger \cdot U^\dagger)(U \cdot V)$ since $(UV)^\dagger = V^\dagger U^\dagger$

$= V^\dagger \cdot (U^\dagger U) \cdot V = V^\dagger \cdot I \cdot V = V^\dagger \cdot V = I$

$\therefore UV$ is unitary

$\therefore$ The product of two unitary matrices is unitary.

Question 5. For any complex $N \times N$ matrix U, we can uniquely write $U = R + iQ$, where R and Q have real entries. Show that if U is unitary, then so is the $2N \times 2N$ matrix U' given in block form by

$$U' = \begin{pmatrix} R & Q \\ -Q & R \end{pmatrix}$$

Thus, by doubling the dimension, we can remove the need for complex-number entries. Show the result of applying this construction to the Pauli matrix Y.

To show that U' is unitary, we need to prove that $U'U'^{\dagger} = U'^{\dagger}U = I$

$U' = \begin{pmatrix} R & Q \\ -Q & R \end{pmatrix}$ $\quad$ $U'^{\dagger} = \begin{pmatrix} R^{\dagger} & -Q^{\dagger} \\ Q^{\dagger} & R^{\dagger} \end{pmatrix}$

$$U'U'^{\dagger} = \begin{pmatrix} R & Q \\ -Q & R \end{pmatrix}\begin{pmatrix} R^{\dagger} & -Q^{\dagger} \\ Q^{\dagger} & R^{\dagger} \end{pmatrix} = \begin{pmatrix} RR^{\dagger} + QQ^{\dagger} & -RQ^{\dagger} + QR^{\dagger} \\ -QR^{\dagger} + RQ^{\dagger} & QQ^{\dagger} + RR^{\dagger} \end{pmatrix}$$

$$U'^{\dagger}U' = \begin{pmatrix} R^{\dagger} & -Q^{\dagger} \\ Q^{\dagger} & R^{\dagger} \end{pmatrix}\begin{pmatrix} R & Q \\ -Q & R \end{pmatrix} = \begin{pmatrix} R^{\dagger}R + Q^{\dagger}Q & R^{\dagger}Q - Q^{\dagger}R \\ Q^{\dagger}R - R^{\dagger}Q & Q^{\dagger}Q + R^{\dagger}R \end{pmatrix}$$

Since $U = R + iQ$ and U is unitary, $UU^{\dagger} = U^{\dagger}U = I$.

$$UU^{\dagger} = (R + iQ)(R^{\dagger} - iQ^{\dagger}) = RR^{\dagger} - RiQ^{\dagger} + iQR^{\dagger} + (iQ)(-iQ^{\dagger})$$
$$= RR^{\dagger} - i(RQ^{\dagger} - QR^{\dagger}) + QQ^{\dagger} = I.$$

$\therefore RR^{\dagger} + QQ^{\dagger} = I$, $\quad RQ^{\dagger} - QR^{\dagger} = 0$

$$\therefore U'U'^{\dagger} = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} = I$$

$$U^{\dagger}U = (R^{\dagger} - iQ^{\dagger})(R + iQ) = R^{\dagger}R + R^{\dagger}iQ - iQ^{\dagger}R + (-iQ^{\dagger})(iQ)$$
$$= R^{\dagger}R - i(R^{\dagger}Q - Q^{\dagger}R) + Q^{\dagger}Q = I$$

$\therefore R^{\dagger}R + Q^{\dagger}Q = I$, $\quad R^{\dagger}Q - Q^{\dagger}R = 0$

$\therefore U'^{\dagger}U' = \begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix} = I$ $\qquad$ $\therefore U'$ is unitary

Pauli matrix $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\quad Y = R + iQ$

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

$$Y' = \begin{bmatrix} R & Q \\ -Q & R \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \qquad Y'^{\dagger} = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}$$

Since $Y' = Y'^{\dagger}$,

$$Y'^{\dagger} Y' = Y' Y'^{\dagger} = \begin{bmatrix} (-1)(-1) & 0 & 0 & 0 \\ 0 & 1\cdot 1 & 0 & 0 \\ 0 & 0 & 1\cdot 1 & 0 \\ 0 & 0 & 0 & (-1)(-1) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I$$

$\therefore$ Y' is unitary.

Question 6. Show that the four Pauli matrices X, Y, Z, I form an orthonormal basis for the space of 2×2 matrices. Thus, we can regard the space of 2×2 matrices as a 4-dimensional complex Hilbert space.

Linearly independent:

$$aX + bY + cZ + dI = 0$$

$$a\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + b\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} + c\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + d\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix} + \begin{pmatrix} 0 & -ib \\ ib & 0 \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & -c \end{pmatrix} + \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix}$$

$$= \begin{pmatrix} c+d & a-ib \\ a+ib & -c+d \end{pmatrix}$$

To make it be equal to the zero matrix,

$$c+d=0 \qquad a-ib=0 \qquad a+ib=0 \qquad -c+d=0$$

$\Rightarrow$ a, b, c, d must be all equal to 0.

$\therefore$ X, Y, Z, I are linearly independent.

Prove the basis is orthonormal: show the Pauli matrices have a unit norm and their inner products are 0.

$$\langle A, B\rangle = \frac{1}{2}\mathrm{Tr}(A^\dagger B), \qquad \|A\| = \langle A, A\rangle^{\frac{1}{2}}$$

$$\langle X, X\rangle = \frac{1}{2}\mathrm{Tr}(X^\dagger X) = \frac{1}{2}\mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\cdot 2 = 1. \quad \|X\| = \langle X, X\rangle^{\frac{1}{2}} = 1.$$

$$\langle Y, Y\rangle = \frac{1}{2}\mathrm{Tr}(Y^\dagger Y) = \frac{1}{2}\mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1, \quad \|Y\| = \langle Y, Y\rangle^{\frac{1}{2}} = 1$$

$$\langle Z, Z\rangle = \frac{1}{2}\mathrm{Tr}(Z^\dagger Z) = \frac{1}{2}\mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1, \quad \|Z\| = \langle Z, Z\rangle^{\frac{1}{2}} = 1$$

$$\langle I, I\rangle = \frac{1}{2}\mathrm{Tr}(I^\dagger I) = \frac{1}{2}\mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1, \quad \|I\| = \langle I, I\rangle^{\frac{1}{2}} = 1$$

$$\langle X, Y\rangle = \frac{1}{2}\mathrm{Tr}(X^\dagger Y) = \frac{1}{2}\mathrm{Tr}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \frac{1}{2}\mathrm{Tr}\begin{pmatrix} (1+0i)(0+i) & 0 \\ 0 & (1+0i)(0-i) \end{pmatrix}$$

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

$$\langle X, Z\rangle = \tfrac{1}{2}\mathrm{Tr}(X^\dagger Z) = \tfrac{1}{2}\mathrm{Tr}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) = \tfrac{1}{2}\mathrm{Tr}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = 0$$

$$\langle X, I\rangle = \tfrac{1}{2}\mathrm{Tr}(X^\dagger I) = \tfrac{1}{2}\mathrm{Tr}\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \tfrac{1}{2}\mathrm{Tr}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 0$$

$$\langle Y, Z\rangle = \tfrac{1}{2}\mathrm{Tr}(Y^\dagger Z) = \tfrac{1}{2}\mathrm{Tr}\left(\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) = \tfrac{1}{2}\mathrm{Tr}\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

$$\langle Y, I\rangle = \tfrac{1}{2}\mathrm{Tr}(Y^\dagger I) = \tfrac{1}{2}\mathrm{Tr}\left(\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right) = \tfrac{1}{2}\mathrm{Tr}\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$$

$$\langle Z, I\rangle = \tfrac{1}{2}\mathrm{Tr}(Z^\dagger I) = \tfrac{1}{2}\mathrm{Tr}\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \tfrac{1}{2}\mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \tfrac{1}{2}(1+(-1)) = 0$$

$\therefore$ All these matrices have a unit norm and their inner products of each other are 0.

$\therefore$ The basis is orthonormal.

$\therefore$ X, Y, Z, I form an orthonormal basis for the space of 2x2 matrices.