

QT207: Introduction to Quantum Computation

Assignment 1 — Shaukat Aziz (22171) — September 4, 2025

Problem 1

Let $\{|\varphi_1\rangle, \dots, |\varphi_n\rangle\}$ and $\{|\psi_1\rangle, \dots, |\psi_n\rangle\}$ be orthonormal bases of a finite-dimensional vector space V . Define

$$U = \sum_{i=1}^n |\psi_i\rangle\langle\varphi_i|$$

1. Show that U is unitary, i.e., $U^\dagger U = I$.

$$\begin{aligned} U^\dagger U &= \left(\sum_{i=1}^n |\varphi_i\rangle\langle\psi_i| \right) \left(\sum_{j=1}^n |\psi_j\rangle\langle\varphi_j| \right) \\ &= \sum_{i,j=1}^n |\varphi_i\rangle\langle\psi_i|\psi_j\rangle\langle\varphi_j| \end{aligned}$$

Since $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ (orthonormality),

$$\begin{aligned} &= \sum_{i=1}^n |\varphi_i\rangle\langle\varphi_i| \\ &= I \end{aligned}$$

Thus, U is unitary.

2. Show that $U|\varphi_j\rangle = |\psi_j\rangle$ for all j .

$$\begin{aligned} U|\varphi_j\rangle &= \sum_{i=1}^n |\psi_i\rangle\langle\varphi_i|\varphi_j\rangle \\ &= \sum_{i=1}^n |\psi_i\rangle\delta_{ij} \quad (\text{since } \langle\varphi_i|\varphi_j\rangle = \delta_{ij}) \\ &= |\psi_j\rangle \end{aligned}$$

So U maps each $|\varphi_j\rangle$ to $|\psi_j\rangle$.

Problem 2

Let H be Hermitian and U be unitary.

1. All eigenvalues of U have unit modulus.

$U|u\rangle = \lambda|u\rangle \implies \langle u|U^\dagger = \langle u|\lambda^*$ where λ & λ^* are the eigenvalues of U and U^\dagger respectively.

$$\begin{aligned}\langle u|U^\dagger U|u\rangle &= \langle u|U^\dagger \lambda|u\rangle = \langle u|\lambda^* \lambda|u\rangle \\ \langle u|I|u\rangle &= \langle u||\lambda|^2|u\rangle = |\lambda|^2 \langle u|u\rangle \\ \langle u|u\rangle &= |\lambda|^2 \langle u|u\rangle \implies |\lambda|^2 = 1\end{aligned}$$

Since λ is a complex number and the only condition is the magnitude = 1, we can write $\lambda = e^{i\phi}$ for some **real** ϕ .

Each unitary U can be written as $U = \exp(iH)$ for some Hermitian H .

We will be using the following properties to prove the above :

- Unitary matrix U is diagonalizable and can be written as $U = V^{-1}DV$ for some diagonal matrix D and the Diagonal matrix contains all the eigen values of U .
- Exponent of a diagonal matrix is the diagonal matrix of the exponents, i.e., if $D = \text{diag}(d_1, d_2, \dots, d_n)$, then $\exp(D) = \text{diag}(e^{d_1}, e^{d_2}, \dots, e^{d_n})$.
- if $U = V^{-1}DV$, then $\exp(U) = V^{-1} \exp(D)V$.
- For a Hermitian matrix $H^\dagger = H$ and eigenvalues of H are real, diagonalizable via unitary transformation i.e $H = WD'W^{-1}$ where D' is diagonal matrix with real eigenvalues.

Let U be a unitary matrix with eigen values $\lambda_j = e^{i\phi_j}$ $j = 1 \dots n$.

Defining : $D' = \text{diag}(\phi_j)$ & $D = \text{diag}(e^{i\phi_j}) \implies \exp(iD') = D$

Then:

$$\begin{aligned}U &= V^{-1}DV = V^{-1} \exp(iD')V \\ \text{Let } H &= V^{-1}D'V \implies \exp(iH) = V^{-1} \exp(iD')V \\ &\implies U = \exp(iH)\end{aligned}$$

The Above H is Hermitian as the matrix is a diagonalizable matrix with real eigen values ϕ_j .

2. Two eigenvectors of U with different eigenvalues are orthogonal.

Let $U|u_1\rangle = \lambda_1|u_1\rangle$ and $U|u_2\rangle = \lambda_2|u_2\rangle$ with $\lambda_1 \neq \lambda_2$. Consider

$$\begin{aligned}\langle u_1|(U|u_2\rangle) &= \lambda_2 \langle u_1|u_2\rangle \\ (\langle u_1|U)|u_2\rangle &= \lambda_1 \langle u_1|u_2\rangle \\ \implies (\lambda_1 - \lambda_2) \langle u_1|u_2\rangle &= 0\end{aligned}$$

In the above we have use $\langle u_1 | U = \langle u_1 | \lambda_1$ because:

$$\begin{aligned} \langle u_1 | U^\dagger &= \langle u_1 | \lambda_1^* \\ \implies \langle u_1 | U^\dagger U &= \lambda_1^* \langle u_1 | U \\ \text{But } U^\dagger U &= I \implies \langle u_1 | U = \frac{1}{\lambda_1^*} \langle u_1 | \\ \text{Since } |\lambda_1|^2 &= 1 \implies \lambda_1^* = \lambda_1^{-1} \\ \implies \langle u_1 | U &= \lambda_1 \langle u_1 | \end{aligned}$$

Since $\lambda_1 \neq \lambda_2$, $\langle u_1 | u_2 \rangle = 0$. Thus, eigenvectors with distinct eigenvalues are orthogonal.

Similarly for Hermitian H : If $H|v_1\rangle = \mu_1|v_1\rangle$, $H|v_2\rangle = \mu_2|v_2\rangle$, $\mu_1 \neq \mu_2$, then using $\langle v_1 | H = \mu_1 \langle v_1 |$ as $H = H^\dagger$:

$$\begin{aligned} \langle v_1 | (H|v_2\rangle) &= \mu_2 \langle v_1 | v_2 \rangle \\ \langle (v_1 | H) | v_2 \rangle &= \mu_1 \langle v_1 | v_2 \rangle \\ \implies (\mu_1 - \mu_2) \langle v_1 | v_2 \rangle &= 0 \end{aligned}$$

So $(\mu_1 - \mu_2) \langle v_1 | v_2 \rangle = 0$. If $\mu_1 \neq \mu_2$, $\langle v_1 | v_2 \rangle = 0 \implies$ eigenvectors with distinct eigenvalues are orthogonal.

3. All columns of U are orthonormal.

if U_i is the column of a matrix U then

$$U = \begin{bmatrix} | & | & & | \\ U_1 & U_2 & \cdots & U_n \\ | & | & & | \end{bmatrix}$$

$$I = (U^\dagger U)_{ij} = \sum_k (U^\dagger)_{ik} U_{kj} = \sum_k U_{ki}^* U_{kj} = \langle U_i | U_j \rangle = \delta_{ij}$$

The above is orthonormality condition for column and for rows:

$$U = \begin{bmatrix} - & R_1 & - \\ - & R_2 & - \\ \vdots & & \\ - & R_n & - \end{bmatrix}$$

$$I = (UU^\dagger)_{ij} = \sum_k U_{ik} U_{jk}^* = R_i R_j^* = \delta_{ij}$$

Problem 3

Let P be a linear operator on a finite-dimensional complex inner-product space V with $P^2 = P$.

1. All eigenvalues of P are 0 or 1.

$$\begin{aligned}
 P|v\rangle &= \lambda|v\rangle \\
 P^2|v\rangle &= P(P|v\rangle) = P(\lambda|v\rangle) = \lambda P|v\rangle = \lambda^2|v\rangle \\
 \implies P^2|v\rangle &= P|v\rangle = \lambda|v\rangle \\
 \implies \lambda^2 &= \lambda \implies \lambda = 0 \text{ or } 1
 \end{aligned}$$

To prove P is diagonalizable: We will be using a property of jordan matrix J that if $J^2 = J$, then J is diagonal matrix. Also, Any matrix can be expressed in terms of its Jordan form:

$$P = YJY^{-1} \implies P^2 = YJY^{-1}YJY^{-1} = YJ^2Y^{-1} = YJY^{-1} = P \implies J^2 = J$$

Since $J^2 = J$, J is diagonal matrix. Hence P is diagonalizable.

2. The complementary operator $Q = I - P$ is also a projector.

$$\begin{aligned}
 Q^2 &= (I - P)(I - P) = I - 2P + P^2 \\
 &= I - 2P + P = I - P = Q
 \end{aligned}$$

3. If $\{|u_i\rangle\}_{i=1}^r$ is an orthonormal set, then $P = \sum_{i=1}^r |u_i\rangle\langle u_i|$ is a projector.

$$\begin{aligned}
 P^2 &= \left(\sum_{i=1}^r |u_i\rangle\langle u_i| \right)^2 \\
 &= \sum_{i,j=1}^r |u_i\rangle\langle u_i| |u_j\rangle\langle u_j| \\
 &= \sum_{i,j=1}^r |u_i\rangle\delta_{ij}\langle u_j| \quad (\text{since } \langle u_i|u_j\rangle = \delta_{ij}) \\
 &= \sum_{i=1}^r |u_i\rangle\langle u_i| = P
 \end{aligned}$$

Problem 4

The Pauli matrices are:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

They are Hermitian, unitary, and traceless. Prove:

1. Squares and inverses: $\sigma_k^2 = I$ and $\sigma_k^{-1} = \sigma_k$ $k = x, y, z$. Since σ_k are Hermitian and Unitary, $\sigma_k^\dagger = \sigma_k = \sigma_k^{-1}$.

$$\implies \sigma_k = \sigma_k^{-1} \implies \sigma_k^2 = I$$

2. Commutators and anticommutators: $[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$ and $\{\sigma_i, \sigma_j\} = 2\delta_{ij}I$. We will use the property : $\sigma_i\sigma_j = -\sigma_j\sigma_i$ if $i \neq j$.

Commutators:

$$\begin{aligned} [\sigma_x, \sigma_y] &= \sigma_x\sigma_y - \sigma_y\sigma_x = i\sigma_z - (-i\sigma_z) = 2i\sigma_z \\ [\sigma_y, \sigma_z] &= 2i\sigma_x, \quad [\sigma_z, \sigma_x] = 2i\sigma_y \\ \implies [\sigma_i, \sigma_j] &= 2i\epsilon_{ijk}\sigma_k \end{aligned}$$

Anticommutators:

$$\begin{aligned} \{\sigma_x, \sigma_y\} &= \sigma_x\sigma_y + \sigma_y\sigma_x = 0 \\ \{\sigma_i, \sigma_i\} &= \sigma_i\sigma_i + \sigma_i\sigma_i = 2\sigma_i^2 = 2I \\ \implies \{\sigma_i, \sigma_j\} &= \sigma_i\sigma_j + \sigma_j\sigma_i = 2\delta_{ij}I \end{aligned}$$

3. Product identity: $\sigma_i\sigma_j = \delta_{ij}I + i\epsilon_{ijk}\sigma_k$.

$$\begin{aligned} \sigma_i\sigma_j &= \frac{1}{2}([\sigma_i, \sigma_j] + \{\sigma_i, \sigma_j\}) \\ &= \frac{1}{2}(2i\epsilon_{ijk}\sigma_k + 2\delta_{ij}I) \\ &= \delta_{ij}I + i\epsilon_{ijk}\sigma_k \end{aligned}$$

For example, $\sigma_x\sigma_y = i\sigma_z$, $\sigma_y\sigma_x = -i\sigma_z$, and $\sigma_i\sigma_i = I$.

4. Vector identities for $\mathbf{a}, \mathbf{b}, \boldsymbol{\sigma} \in \mathbb{R}^3$:

Define:

- $\mathbf{a} = (a_1, a_2, a_3)$
- $\mathbf{b} = (b_1, b_2, b_3)$
- $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ (by definition)

We will Prove first that $(\mathbf{a} \cdot \boldsymbol{\sigma})(\mathbf{b} \cdot \boldsymbol{\sigma}) = (\mathbf{a} \cdot \mathbf{b})I + i(\mathbf{a} \times \mathbf{b}) \cdot \boldsymbol{\sigma}$:

$$\begin{aligned} (\mathbf{a} \cdot \boldsymbol{\sigma})(\mathbf{b} \cdot \boldsymbol{\sigma}) &= \sum_i a_i \sigma_i \sum_j b_j \sigma_j = \sum_{i,j} a_i b_j \sigma_i \sigma_j \\ &= \sum_{i,j} a_i b_j (\delta_{ij}I + i\epsilon_{ijk}\sigma_k) \quad (\because \sigma_i \sigma_j = \delta_{ij}I + i\epsilon_{ijk}\sigma_k) \\ &= \sum_i a_i b_i + i \sum_{i,j} a_i b_j \epsilon_{ijk} \sigma_k \\ &= (\mathbf{a} \cdot \mathbf{b})I + i(\mathbf{a} \times \mathbf{b}) \cdot \boldsymbol{\sigma} \end{aligned}$$

Now taking $\mathbf{a} = \mathbf{b}$, we find:

$$\begin{aligned} (\mathbf{a} \cdot \boldsymbol{\sigma})^2 &= (\mathbf{a} \cdot \boldsymbol{\sigma})(\mathbf{a} \cdot \boldsymbol{\sigma}) \\ &= (\mathbf{a} \cdot \mathbf{a})I + i(\mathbf{a} \times \mathbf{a}) \cdot \boldsymbol{\sigma} \\ &= |\mathbf{a}|^2 I + 0 \\ &= |\mathbf{a}|^2 I \end{aligned}$$

Problem 5

A density operator ρ on a finite-dimensional Hilbert space \mathcal{H} for an ensemble $\{p_i, |\psi_i\rangle\}$ is $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Prove:

1. ρ is Hermitian, positive semidefinite, and $\text{Tr}(\rho) = 1$.

$$\begin{aligned}\rho^\dagger &= \sum_i p_i (|\psi_i\rangle\langle\psi_i|)^\dagger = \sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho && (\implies \rho \text{ is Hermitian}) \\ \langle\phi|\rho|\phi\rangle &= \sum_i p_i \langle\phi|\psi_i\rangle\langle\psi_i|\phi\rangle = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0 && (\implies \rho \text{ is positive semidefinite}) \\ \text{Tr}(\rho) &= \sum_i p_i \text{Tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i |\psi_i|^2 = 1 && (\implies \text{Tr}(\rho) = 1)\end{aligned}$$

In the above: $p_i \geq 0$ as it is probability and $|\langle\phi|\psi_i\rangle|^2 \geq 0$, $\text{Tr}(|a\rangle\langle a|) = \langle a|a\rangle$.

2. $0 \leq \text{Tr}(\rho^2) \leq 1$ and ρ represents a pure state $\iff \rho^2 = \rho \implies \text{Tr}(\rho^2) = 1$.

$$\begin{aligned}\text{Tr}(\rho^2) &= \text{Tr} \left(\sum_{i,j} p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j| \right) \\ &= \sum_{i,j} p_i p_j \text{Tr} (|\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j|) \\ &= \sum_{i,j} p_i p_j \langle\psi_i|\psi_j\rangle \text{Tr} (|\psi_j\rangle\langle\psi_i|) \\ &= \sum_{i,j} p_i p_j |\langle\psi_i|\psi_j\rangle|^2 \leq \sum_{i,j} p_i p_j = (\sum_i p_i)^2 = 1\end{aligned}$$

For pure states, $\rho = |\psi\rangle\langle\psi|$, $\rho^2 = \rho$, $\text{Tr}(\rho^2) = 1$. For mixed states, $\text{Tr}(\rho^2) < 1$. Like above, we can see that the inequality becomes strict for mixed states.

3. **Spectral form:** $\rho = \sum_k \lambda_k |\phi_k\rangle\langle\phi_k|$, $\lambda_k \geq 0$, $\sum_k \lambda_k = 1$. **Probabilities are λ_k .**

$$\begin{aligned}\text{Tr}(\rho^2) &= \text{Tr} \left(\sum_{k,l} \lambda_k \lambda_l |\phi_k\rangle\langle\phi_k|\phi_l\rangle\langle\phi_l| \right) \\ &= \sum_{k,l} \lambda_k \lambda_l \delta_{k,l} \text{Tr} (|\phi_l\rangle\langle\phi_k|) && (\because \langle\phi_k|\phi_l\rangle = \delta_{k,l} \text{ (orthonormality)}) \\ &= \sum_k \lambda_k^2 \langle\phi_k|\phi_k\rangle \\ &= \sum_k \lambda_k^2 = 1 && (\because \rho^2 = \rho) \text{ as orthonormal basis } |\phi_k\rangle \text{ is used for spectral decomposition}\end{aligned}$$

ρ here a pure state which was defined as $\rho = \sum_k |\phi_k\rangle\langle\phi_k|$ where $|\phi_k\rangle$ are orthonormal .

4. Expectation values: For observable A , $\langle A \rangle = \text{Tr}(\rho A) = \sum_i p_i \langle \psi_i | A | \psi_i \rangle$.

$$\langle A \rangle = \langle \psi | A | \psi \rangle \text{ and } |\psi\rangle = \sum_i \sqrt{p_i} |\psi_i\rangle \quad (\text{Definition})$$

$$\langle A \rangle = \sum_i p_i \langle \psi_i | A | \psi_i \rangle = \sum_i p_i \text{Tr}(|\psi_i\rangle \langle \psi_i| A) = \text{Tr}(\rho A)$$

Problem 6

In finite dimensions, positivity of an operator X means $\langle \psi | X | \psi \rangle \geq 0$ for all $|\psi\rangle$. Prove:

1. A positive operator is Hermitian.

Proof. Write A as $A = B + iC$ where $B = (A + A^\dagger)/2$ and $C = (A - A^\dagger)/(2i)$ are Hermitian. For any vector $|\psi\rangle$,

$$\langle \psi | A | \psi \rangle = \langle \psi | B | \psi \rangle + i \langle \psi | C | \psi \rangle.$$

By hypothesis the left-hand side is real and nonnegative for every $|\psi\rangle$, so its imaginary part must vanish for all $|\psi\rangle$, i.e.

$$\langle \psi | C | \psi \rangle = 0 \quad \text{for all } |\psi\rangle.$$

Since C is Hermitian, it admits a spectral decomposition:

$$C = \sum_k c_k |\phi_k\rangle \langle \phi_k|$$

where c_k are real eigenvalues and $|\phi_k\rangle$ are orthonormal eigenvectors. Setting $|\psi\rangle = |\phi_k\rangle$ gives

$$\langle \phi_k | C | \phi_k \rangle = c_k = 0 \quad \text{for all } k.$$

Therefore, all eigenvalues vanish and $C = 0$. Thus, $A = B$ is Hermitian. \square

2. For any linear operator A , the operator $A^\dagger A$ is positive and Hermitian.

Proof. For any $|\psi\rangle$,

$$\langle \psi | A^\dagger A | \psi \rangle = \langle A\psi | A\psi \rangle = \|A\psi\|^2 \geq 0,$$

so $A^\dagger A$ is positive. Moreover $(A^\dagger A)^\dagger = A^\dagger (A^\dagger)^\dagger = A^\dagger A$, so it is Hermitian. Consequently all eigenvalues of $A^\dagger A$ are real and nonnegative. \square

Problem 7

For matrices $A \in \mathbb{C}^{m \times n}$, $C \in \mathbb{C}^{n \times p}$, $B \in \mathbb{C}^{k \times \ell}$, and $D \in \mathbb{C}^{\ell \times q}$, prove the mixed-product property:

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD).$$

Proof. Let $A \in \mathbb{C}^{m \times n}$, $C \in \mathbb{C}^{n \times p}$, $B \in \mathbb{C}^{k \times \ell}$, $D \in \mathbb{C}^{\ell \times q}$. The (i, j) -th block of $(A \otimes B)(C \otimes D)$ is:

$$\sum_{r=1}^n (a_{ir}B)(c_{rj}D).$$

Since scalars commute with matrices, we can regroup:

$$\sum_{r=1}^n (a_{ir}c_{rj})(BD).$$

Thus the (i, j) -th block of $(A \otimes B)(C \otimes D)$ is:

$$\left(\sum_{r=1}^n a_{ir}c_{rj} \right) BD = (AC)_{ij}BD.$$

But this is exactly the (i, j) -th block of $(AC) \otimes (BD)$:

$$(AC) \otimes (BD) = \begin{bmatrix} (AC)_{11}(BD) & \cdots & (AC)_{1p}(BD) \\ \vdots & \ddots & \vdots \\ (AC)_{m1}(BD) & \cdots & (AC)_{mp}(BD) \end{bmatrix}.$$

Therefore,

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD).$$

□