COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Mechanics: Linear Algebra

Spectral Decomposition Theorem

Any normal operator M on a vector space V is a diagonalizable with respect to some orthonormal basis for V. Conversely, any diagononalizable operator is normal.

- Exercise: Show that a normal matrix is Hermitian if and only if it has real eigenvalues.
- Unitary matrix: A matrix U is called unitary if $UU^\dagger = U^\dagger U = I$.
- Unitary operator: An operator U is unitary if $UU^\dagger = U^\dagger U = I$.
- Exercise: Show that unitary operators preserve inner products.
- Exercise: Let $|v_i\rangle$ be any orthonormal basis set and let $|w_i\rangle = U|v_i\rangle$. Then $|w_i\rangle$ is an orthonormal basis set. Moreover, $U = \sum_i |w_i\rangle\langle v_i|$.
- Exercise: If $|v_i\rangle$ and $|w_i\rangle$ are two orthonormal basis sets, then $U \equiv \sum_i |w_i\rangle\langle v_i|$ is a unitary operator.
- Exercise: Show that all the eigenvalues of a unitary matrix have modulus 1. This means that they can be written as $e^{i\theta}$ for some real θ.

- Positive operator: An operator A is said to be a positive operator if for every vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real non-negative number.
- Positive definite operator: An operator A is said to be a positive operator if for every vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real number strictly greater than 0.

- Positive operator: An operator A is said to be a positive operator if for every vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real non-negative number.
- Positive definite operator: An operator A is said to be a positive operator if for every vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real number strictly greater than 0.
- Exercises:
  - Show that a positive operator is necessarily Hermitian.
  - Show that the eigenvectors of a Hermitian operator with different eigenvalues are necessarily orthogonal.
  - Show that for any operator A, $A^{\dagger}A$ is positive.
  - Show that the eigenvalues of a projector P are all either 0 or 1.

- The tensor product is a way of putting vector spaces together to form larger vector spaces.
  - Suppose V and W are Hilbert spaces of dimension m and n respectively, then $V \otimes W$ denotes an mn-dimensional vector space.
  - The elements of $V \otimes W$ are linear combinations of tensor products $|v\rangle \otimes |w\rangle$ of elements $|v\rangle \in V$ and $|w\rangle \in W$.
  - If $|i\rangle$'s and $|j\rangle$'s are orthonormal bases for V and W respectively, then $|i\rangle \otimes |j\rangle$'s are orthonormal basis for $V \otimes W$.
  - $|v\rangle \otimes |w\rangle$ is also written as $|vw\rangle$, $|v\rangle |w\rangle$, and $|v, w\rangle$.
  - Example: If V is a two-dimensional vector space with basis $\{|0\rangle, |1\rangle\}$, then $|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ is an element of $V \otimes V$.
- Notation: $|\psi\rangle^{\otimes k}$ means $|\psi\rangle$ tensored with itself k times.

- Some properties of tensor products:
  - For any arbitrary scalar z and elements $|v\rangle \in V$ and $|w\rangle \in W$:

$$z(|v\rangle \otimes |w\rangle) = (z\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z\,|w\rangle).$$

  - For arbitrary $|v_1\rangle, |v_2\rangle \in V$ and $|w\rangle \in W$,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle.$$

  - For arbitrary $|v\rangle \in V$ and $|w_1\rangle, |w_2\rangle \in W$,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle.$$

- Linear operators on $V \otimes W$: Let A and B be linear operators on V and W respectively. Then $A \otimes B$ denotes a linear operator on $V \otimes W$ defined as:

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle .$$

  Furthermore, the following ensures linearity:

$$(A \otimes B)\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle\right) = \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle .$$

- Let $A : V \to V'$ and $B : W \to W'$ be linear operators. An arbitrary linear operator C mapping $V \otimes W$ to $V' \otimes W'$ can be represented as a linear combination:

$$C = \sum_i c_i A_i \otimes B_i$$

  where by definition:

$$\left(\sum_i c_i A_i \otimes B_i\right)|v\rangle \otimes |w\rangle \equiv \sum_i c_i A_i |v\rangle \otimes B_i |w\rangle .$$

- Linear operators on $V \otimes W$: Let A and B be linear operators on V and W respectively. Then $A \otimes B$ denotes a linear operator on $V \otimes W$ defined as:

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle .$$

Furthermore, the following ensures linearity:

$$(A \otimes B)\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle\right) = \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle .$$

- Let $A : V \rightarrow V'$ and $B : W \rightarrow W'$ be linear operators. An arbitrary linear operator C mapping $V \otimes W$ to $V' \otimes W'$ can be represented as a linear combination:

$$C = \sum_i c_i A_i \otimes B_i$$

where by definition:
$(\sum_i c_i A_i \otimes B_i)|v\rangle \otimes |w\rangle \equiv \sum_i c_i A_i |v\rangle \otimes B_i |w\rangle$.
- The inner product on $V \otimes W$ is defined as:

$$\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j |v_j'\rangle \otimes |w_j'\rangle\right) \equiv \sum_{ij} a_i^* b_j \langle v_i | v_j'\rangle \langle w_j | w_j'\rangle .$$

- Matrix representation: The matrix representation for $A \otimes B$ is called the Kronecker product. Let A be a $m \times n$ matrix and B be a $p \times q$ matrix. Then the matrix representation of $A \otimes B$ is given as:

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21} & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}$$

  - Example: What is $\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix}$?

- Matrix representation: The matrix representation for $A \otimes B$ is called the Kronecker product. Let A be a $m \times n$ matrix and B be a $p \times q$ matrix. Then the matrix representation of $A \otimes B$ is given as:

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21} & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}$$

  - Example: What is $\begin{bmatrix} 1 \\ 2 \end{bmatrix} \otimes \begin{bmatrix} 2 \\ 3 \end{bmatrix}$? $\begin{bmatrix} 2 \\ 3 \\ 4 \\ 6 \end{bmatrix}$

- Exercises:
  - Show that $(A \otimes B)^* = A^* \otimes B^*; (A \otimes B)^T = A^T \otimes B^T; (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.
  - Show that the tensor product of two unitary operators is unitary.
  - Show that the tensor product of two Hermitian operators is Hermitian.
  - Show that the tensor product of two positive operators is postive.
  - Show that the tensor product of two projectors is a projector.

- One can define matrix functions on normal matrices by using the following construction: Let $A = \sum_a a |a\rangle \langle a|$ be a spectral decomposition for a normal operator A. We define:

$$f(A) = \sum_a f(a) |a\rangle \langle a|$$

  - Exercise: Show that $exp(\theta Z) = \begin{bmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{bmatrix}$.
  - Exercise: Find the square root of the matrix $\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}$.

- The postulates of quantum mechanics were derived after a long process of trial and error.

Postulate 1 (State space)

Associated to any isolated physical system is a complex vector space with inner product (Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

Postulate 1 (State space)

Associated to any isolated physical system is a complex vector space with inner product (Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

- Determining the state space of real systems may be complicated and beyond the scope of our discussion.
- We start with a simplest quantum mechanical system (a qubit) that has a two-dimensional state space with $|0\rangle$ and $|1\rangle$ being the orthonormal basis. This system is described by a state vector $|\psi\rangle$ where $\langle\psi|\psi\rangle = 1$.

Postulate 1 (State space)

Associated to any isolated physical system is a complex vector space with inner product (Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

- Determining the state space of real systems may be complicated and beyond the scope of our discussion.
- We start with a simplest quantum mechanical system (a qubit) that has a two-dimensional state space with $|0\rangle$ and $|1\rangle$ being the orthonormal basis. This system is described by a state vector $|\psi\rangle$ where $\langle\psi|\psi\rangle = 1$.

Postulate 2 (Evolution)

The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which only depends on the times t_1 and t_2, $|\psi'\rangle = U|\psi\rangle$.

- Doesn't applying a unitary gate contradict with the system being closed?

Postulate 3 (Measurement)

Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The following properties hold:

- The index m refers to the measurement outcomes that may occur in the experiment.
- If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that the result m occurs is given by
$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$
and the state of the system after the measurement is given by
$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}$$
- The measurement operators satisfy the *completeness equation*,
$$\sum_m M_m^\dagger M_m = I$$
.

Postulate 3 (Measurement)

Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The following properties hold:

- The index m refers to the measurement outcomes that may occur in the experiment.
- If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that the result m occurs is given by $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$, and the state of the system after the measurement is given by $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$
- The measurement operators satisfy the *completeness equation*, $\sum_m M_m^\dagger M_m = I$.

- <u>Exercise</u>: Show that $\sum_m p(m) = 1$.

Postulate 3 (Measurement)

Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The following properties hold:

- The index m refers to the measurement outcomes that may occur in the experiment.
- If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that the result m occurs is given by $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$, and the state of the system after the measurement is given by $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$
- The measurement operators satisfy the *completeness equation*, $\sum_m M_m^\dagger M_m = I$.

- Exercise: Consider a single-qubit scenario with measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Compare the above properties with what we did in earlier lectures.

Postulate 3 (Measurement)

Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The following properties hold:

- The index m refers to the measurement outcomes that may occur in the experiment.
- If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that the result m occurs is given by $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$, and the state of the system after the measurement is given by $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$
- The measurement operators satisfy the *completeness equation*, $\sum_m M_m^\dagger M_m = I$.

- Cascaded measurements: Suppose $\{L_l\}$ and $\{M_m\}$ are two sets of measurement operators. Show that a measurement defined by the measurement operators $\{L_l\}$ followed by $\{M_m\}$ is physically equivalent to a single measurement defined by the measurement operators $\{N_{lm}\}$ where $N_{lm} = M_m L_l$.

- We hinted earlier that distinguishing non-orthogonal states may not be possible. Now that we understands measurements, let us try to formulate and prove.
- The ability to distinguish quantum states can be formalised as the following game between two parties:

Distinguishing quantum states

Alice chooses a state $|\psi_i\rangle$ from a fixed set of states $|\psi_1\rangle, ..., |\psi_n\rangle$ (known to both Alice and Bob) and gives this state to Bob whose task is to identify i.

- Claim 1: There is a winning strategy for Bob if $|\psi_1\rangle, ..., |\psi_n\rangle$ are orthonormal states.
- Claim 2: There is no winning strategy for Bob if there are non-orthogonal states.

Distinguishing quantum states

Alice chooses a state $|\psi_i\rangle$ from a fixed set of states $|\psi_1\rangle, \ldots, |\psi_n\rangle$ (known to both Alice and Bob) and gives this state to Bob whose task is to identify i.

- Claim 1: There is a winning strategy for Bob if $|\psi_1\rangle, \ldots, |\psi_n\rangle$ are orthonormal states.
  - Define measurement operators $M_i = |\psi_i\rangle \langle\psi_i|$.
  - Define $M_0 = \sqrt{I - \sum_{i=1}^{n} M_i}$. Note that since $I - \sum_{i=1}^{n} M_i$ is a positive operator, square root is well defined.
  - Claim 1.1: $M_0, M_1, \ldots, M_n$ satisfy completeness relation.
  - Claim 1.2: Given state $|\psi_i\rangle$, $p(i) = 1$.

Distinguishing quantum states

Alice chooses a state $|\psi_i\rangle$ from a fixed set of states $|\psi_1\rangle, ..., |\psi_n\rangle$ (known to both Alice and Bob) and gives this state to Bob whose task is to identify i.

- Claim 2: There is no winning strategy for Bob if there are non-orthogonal states.

Proof sketch

- Assume $n = 2$ and let $|\psi_1\rangle$ and $|\psi_2\rangle$ be non-orthogonal.
- The most general strategy for Bob is to measure using operators $\{M_m\}$ and use a function $f : \{1, ..., m\} \rightarrow \{1, 2\}$ to return an answer to Alice. Suppose for the sake of contradiction, there exists such a winning strategy for Bob.
- Let $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$ for $i = 1, 2$.
- Since this is a winning strategy for Bob, we have:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1$$

Distinguishing quantum states

Alice chooses a state $|\psi_i\rangle$ from a fixed set of states $|\psi_1\rangle, ..., |\psi_n\rangle$ (known to both Alice and Bob) and gives this state to Bob whose task is to identify i.

- Claim 2: There is no winning strategy for Bob if there are non-orthogonal states.

Proof sketch

- Assume $n = 2$ and let $|\psi_1\rangle$ and $|\psi_2\rangle$ be non-orthogonal.
- The most general strategy for Bob is to measure using operators $\{M_m\}$ and use a function $f : \{1, ..., m\} \rightarrow \{1, 2\}$ to return an answer to Alice. Suppose for the sake of contradiction, there exists such a winning strategy for Bob.
- Let $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$ for $i = 1, 2$.
- Since this is a winning strategy for Bob, we have: $\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1$
- Claim 2.1: $\sqrt{E_2} |\psi_1\rangle = 0$

Distinguishing quantum states

Alice chooses a state $|\psi_i\rangle$ from a fixed set of states $|\psi_1\rangle, ..., |\psi_n\rangle$ (known to both Alice and Bob) and gives this state to Bob whose task is to identify i.

- Claim 2: There is no winning strategy for Bob if there are non-orthogonal states.

Proof sketch

- Assume $n = 2$ and let $|\psi_1\rangle$ and $|\psi_2\rangle$ be non-orthogonal.
- The most general strategy for Bob is to measure using operators $\{M_m\}$ and use a function $f : \{1, ..., m\} \rightarrow \{1, 2\}$ to return an answer to Alice. Suppose for the sake of contradiction, there exists such a winning strategy for Bob.
- Let $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$ for $i = 1, 2$.
- Since this is a winning strategy for Bob, we have: $\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1$
- Claim 2.1: $\sqrt{E_2}\,|\psi_1\rangle = 0$
- Claim 2.2: Decompose $|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\phi\rangle$, where $|\phi\rangle$ is orthonormal to $|\psi_1\rangle$. Then $|\beta| < 1$.

Distinguishing quantum states

Alice chooses a state $|\psi_i\rangle$ from a fixed set of states $|\psi_1\rangle, \ldots., |\psi_n\rangle$ (known to both Alice and Bob) and gives this state to Bob whose task is to identify i.

- Claim 2: There is no winning strategy for Bob if there are non-orthogonal states.

Proof sketch

- Assume $n = 2$ and let $|\psi_1\rangle$ and $|\psi_2\rangle$ be non-orthogonal.
- The most general strategy for Bob is to measure using operators $\{M_m\}$ and use a function $f : \{1, \ldots, m\} \rightarrow \{1, 2\}$ to return an answer to Alice. Suppose for the sake of contradiction, there exists such a winning strategy for Bob.
- Let $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$ for $i = 1, 2$.
- Since this is a winning strategy for Bob, we have: $\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1$
- Claim 2.1: $\sqrt{E_2} |\psi_1\rangle = 0$
- Claim 2.2: Decompose $|\psi_2\rangle = \alpha |\psi_1\rangle + \beta |\phi\rangle$, where $|\phi\rangle$ is orthonormal to $|\psi_1\rangle$. Then $|\beta| < 1$.
- Claim 2.3: $\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\phi| E_2 |\phi\rangle \leq |\beta|^2 < 1$.
- The above contradicts with the fourth bullet item.

End