COL866: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

- 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*, $\sum_m M_m^\dagger M_m = I$.

- Exercise: 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 $|\psi_1\rangle, ..., |\psi_n\rangle$ (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.
  - 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: $M_0, M_1, ..., M_n$ 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:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1, \quad \text{and hence}$$
$$\langle\psi_1| E_2 |\psi_1\rangle = 0; \langle\psi_2| E_1 |\psi_2\rangle = 0$$

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:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1, \quad \text{and hence}$$
$$\langle\psi_1| E_2 |\psi_1\rangle = 0; \langle\psi_2| E_1 |\psi_2\rangle = 0$$

- Claim 2.1: $\sqrt{E_2}\, |\psi_1\rangle = \mathbf{0}$

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:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1, \quad \text{and hence}$$
$$\langle\psi_1| E_2 |\psi_1\rangle = 0; \langle\psi_2| E_1 |\psi_2\rangle = 0$$

- Claim 2.1: $\sqrt{E_2}\,|\psi_1\rangle = \mathbf{0}$
- 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 $|\psi_1\rangle, ..., |\psi_n\rangle$ (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:

$$\langle\psi_1| E_1 |\psi_1\rangle = 1; \langle\psi_2| E_2 |\psi_2\rangle = 1, \quad \text{and hence}$$
$$\langle\psi_1| E_2 |\psi_1\rangle = 0; \langle\psi_2| E_1 |\psi_2\rangle = 0$$

- Claim 2.1: $\sqrt{E_2} |\psi_1\rangle = \mathbf{0}$
- 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