Quantum Computing
Lecture 3

Anuj Dawar

Principles of Quantum Mechanics

What is Quantum Mechanics

Quantum Mechanics is a framework for the development of physical theories.

It is not itself a physical theory.

It states *four mathematical postulates* that a physical theory must satisfy.

Actual physical theories, such as *Quantum Electrodynamics* are built upon a foundation of quantum mechanics.

What are the Postulates About

The four postulates specify a general framework for describing the behaviour of a physical system.

1. How to describe the state of a closed system.—*Statics* or *state space*
2. How to describe the evolution of a closed system.—*Dynamics*
3. How to describe the interactions of a system with external systems.—*Measurement*
4. How to describe the state of a composite system in terms of its component parts.

First Postulate

Associated to any physical system is a *complex inner product space* known as the *state space* of the system.

The system is completely described at any given point in time by its *state vector*, which is a *unit vector* in its state space.

Note: Quantum Mechanics does not prescribe what the state space is for any given physical system. That is specified by individual physical theories.

Example: A Qubit

Any system whose state space can be described by $\mathbb{C}^2$—the two-dimensional complex vector space—can serve as an implementation of a qubit.

Example: An electron spin.

Some systems may require an infinite-dimensional state space.

We always assume, for the purposes of this course, that our systems have a *finite dimensional* state space.

Second Postulate

The time evolution of *closed* quantum system is described by the Schrödinger equation:

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where

- $\hbar$ is Planck's constant; and
- H is a fixed Hermitian operator known as the *Hamiltonian* of the system.

Second Postulate—Simpler Form

The state $|\psi\rangle$ of a closed quantum system at time t_1 is related to the state $|\psi'\rangle$ at time t_2 by a unitary operator U that depends only on t_1 and t_2.

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

U is obtained from the Hamiltonian H by the equation:

$$U(t_1, t_2) = \exp[\frac{-iH(t_2 - t_1)}{\hbar}]$$

This allows us to consider time as discrete and speak of *computational steps*

Exercise: Check that if H is Hermitian, U is unitary.

Why Unitary?

Unitary operations are the only linear maps that preserve norm.

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

implies

$$||\,|\psi'\rangle|| = ||\,U|\psi\rangle|| = ||\,|\psi\rangle|| = 1$$

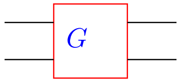
Exercise: Verify that unitary operations are norm-preserving.

Gates, Operators, Matrices

In this course, most linear operators we will be interested in are unitary.

They can be represented as matrices where each column is a *unit vector* and columns are pairwise orthogonal.

Another useful representation of unitary operators we will use is as gates:

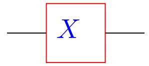


A 2-qubit gate is a unitary operator on $\mathbb{C}^4$.

Pauli Gates

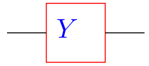
A particularly useful set of 1-*qubit* gates are the *Pauli Gates*.

The X gate



$$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle \; X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

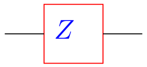
The Y gate



$$Y|0\rangle = i|1\rangle \quad Y|1\rangle = -i|0\rangle \; Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$$

Pauli Gates–contd.

The Z gate



$$Z|0\rangle = |0\rangle \quad Z|1\rangle = -|1\rangle \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Sometimes we include the identity $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ as a fourth Pauli gate.

Third Postulate

A measurement on a quantum system has some set M of outcomes.

Quantum measurements are described by a collection $\{P_m : m \in M\}$ of *measurement operators*. These are linear (not unitary) operators acting on the state space of the system.

If the state of the system is $|\psi\rangle$ before the measurement, then the probability of outcome m is:

$$p(m) = \langle\psi|P_m^\dagger P_m|\psi\rangle$$

The state of the system after measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{\langle\psi|P_m^\dagger P_m|\psi\rangle}}$$

Third Postulate—contd.

The measurement operators satisfy the *completeness equation*.

$$\sum_{m \in M} P_m^\dagger P_m = I$$

This guarantees that the sum of the probabilities of all outcomes adds up to 1.

$$\sum_m p(m) = \sum_m \langle \psi | P_m^\dagger P_m | \psi \rangle = \langle \psi | I | \psi \rangle = 1$$

Measurement in the Computational Basis

We are generally interested in the special case where the measurement operators are projections onto a particular orthonormal basis of the state space (which we call the *computational basis*).

So, for a single qubit, we take measurement operators $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$

This gives, for a qubit in state $\alpha|0\rangle + \beta|1\rangle$:

$$p(0) = |\alpha|^2 \quad p(1) = |\beta|^2$$

Exercise: Verify!

Global Phase

For any state $|\psi\rangle$, and any θ, we can form the vector $e^{i\theta}|\psi\rangle$.

Then, for any unitary operator U,

$$U e^{i\theta} |\psi\rangle = e^{i\theta} U |\psi\rangle$$

Moreover, for any measurement operator P_m

$$\langle \psi | e^{-i\theta} P_m^\dagger P_m e^{i\theta} | \psi \rangle = \langle \psi | P_m^\dagger P_m | \psi \rangle$$

Thus, such a global phase is unobservable and the states are physically indistinguishable.

Relative Phase

In contrast, consider the two states $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
Measured in the computational basis, they yield the same outcome probabilities.

However, measured in a different orthonormal basis (say $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, the results are different.

Also, if $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, then

$$H|\psi_1\rangle = |0\rangle \quad H|\psi_2\rangle = |1\rangle$$

Fourth Postulate

The state space of a composite physical system is the tensor product of the state spaces of the individual component physical systems.

If one component is in state $|\psi_1\rangle$ and a second component is in state $|\psi_2\rangle$, the state of the combined system is

$$|\psi_1\rangle \otimes |\psi_2\rangle$$

Not all states of a combined system can be separated into the tensor product of states of the individual components.

Separable States

A state of a combined system is *separable* if it can be expressed as the tensor product of states of the components.

E.g.

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

If Alice has a system in state $|\psi_1\rangle$ and Bob has a system in state $|\psi_1\rangle$, the state of their combined system is $|\psi_1\rangle \otimes |\psi_1\rangle$.

If Alice applies U to her state, this is equivalent to applying the operator $U \otimes I$ to the combined state.

Entangled States

The following state of a 2-qubit system cannot be separated into components part.

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Note: Physical separation does not imply separability. Two particles that are physically separated could still be entangled.

Summary

Postulate 1: A closed system is described by a unit vector in a complex inner product space.

Postulate 2: The evolution of a closed system in a fixed time interval is described by a unitary transform.

Postulate 3: If we measure the state $|\psi\rangle$ of a system in an orthonormal basis $|0\rangle \cdots |n-1\rangle$, we get the result $|j\rangle$ with probability $|\langle j|\psi\rangle|^2$. After the measurement, the state of the system is the result of the measurement.

Postulate 4: The state space of a composite system is the tensor product of the state spaces of the components.