Quantum Computing
Lecture 3

Postulates of Quantum Mechanics

Maris Ozols

What is quantum mechanics?

Quantum mechanics is a branch of physics that describes the behaviour of systems, such as atoms and photons, whose states admit superpositions.

It is a framework onto which other physical theories are built upon. For example, quantum field theories such as quantum electrodynamics and quantum chromodynamics.

The central topic of this lecture is a mathematical formulation of quantum mechanics consisting of four postulates.

This lecture is based on Section 2.2 of the book by Nielsen & Chuang.

What are the four postulates about?

Open vs closed systems

Closed system is an ideal physical system that does not interact at all with its environment. An open system *does* interact with its environment.

Postulates

They specify a general framework for describing the behaviour of a physical system:

1. **Statics (state space):** describes the state of a closed system
2. **Dynamics:** describes the evolution of a closed system
3. **Measurement:** describes how information is extracted from a closed system via interactions with an external system
4. **Composite systems:** describes the state of a composite system in terms of its component parts

First Postulate

The state space of any *closed* physical system is a complex vector space. At any given point in time, the system is completely described by a state vector, which is a unit vector in its state space.

Note: Quantum mechanics does not prescribe what the state space of a particular physical system is, this is determined by more specific theories.

Any physical system whose state space can be described by $\mathbb{C}^2$ can serve as an implementation of a qubit.

Examples:

- spin of an electron
- polarization of a photon
- current in a superconducting circuit

Some systems may require an infinite-dimensional Hilbert space as their state space. However, for the purpose of this course we always assume that our systems are finite-dimensional.

Second Postulate

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

$$i\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$$

where H is a fixed Hermitian operator known as the Hamiltonian.

By solving this differential equation one gets:

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \qquad \text{where} \qquad U(t) = \exp(-iHt)$$

and $|\psi(0)\rangle$ is the state at $t = 0$. One can check that $U(t)$ is unitary.

While some models (such as adiabatic quantum computing) allow for continuous-time evolution, we consider only discrete computational steps.

The discrete-time evolution of a *closed* quantum system is described by a unitary transformation U:

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

Expressing a state in any basis

Any state $|\psi\rangle \in \mathbb{C}^n$ can be expressed in the standard basis as follows:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \sum_{i=1}^{n} \alpha_i |i\rangle = \sum_{i=1}^{n} \langle i|\psi\rangle |i\rangle$$

where $\alpha_i = \langle i|\psi\rangle$ is the i-th coordinate of $|\psi\rangle$ (in the standard basis).

Similarly, if $\{|u_1\rangle, \ldots, |u_n\rangle\}$ is any other orthonormal basis of $\mathbb{C}^n$, we can express $|\psi\rangle$ in this basis as follows:

$$|\psi\rangle = \sum_{i=1}^{n} \langle u_i|\psi\rangle |u_i\rangle$$

where $\langle u_i|\psi\rangle$ is the i-th coordinate of $|\psi\rangle$ in the basis $\{|u_1\rangle, \ldots, |u_n\rangle\}$.

Unitary change of basis

Let $\{|u_1\rangle, \dots, |u_n\rangle\}$ be some orthonormal basis of $\mathbb{C}^n$. Then we can express any $|\psi\rangle \in \mathbb{C}^n$ in two different ways:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle = \sum_{j=1}^{n} \beta_j |u_j\rangle$$

for some coordinates $\alpha_i, \beta_j \in \mathbb{C}$. How are α_i and β_j related?

If we left-multiply both sides by $\langle i|$, we get

$$\alpha_i = \sum_{j=1}^{n} \beta_j \langle i|u_j\rangle = \sum_{j=1}^{n} M_{ij}\beta_j$$

where $M_{ij} = \langle i|u_j\rangle$. Since this holds for every i,

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

Unitary change of basis (continued)

If we left-multiply by M^{-1}, we get

$$M^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

But we could have done the whole calculation the other way and got

$$N \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

where $N_{ij} = \langle u_i|j\rangle = \overline{\langle j|u_i\rangle} = \overline{M_{ji}}$. We conclude that $M^{-1} = N = M^\dagger$.

In particular, $MM^\dagger = M^\dagger M = I$ so M is unitary! The same holds for N.

Unitary change of basis (continued 2)

Since N allows us to compute from α_i the new coordinates β_j, we can use it to convert any vector from the standard basis $\{|1\rangle, \dots, |n\rangle\}$ to the new basis $\{|u_1\rangle, \dots, |u_n\rangle\}$.

Recall that $N_{ij} = \langle u_i|j\rangle$, so we can write N explicitly as follows:

$$N = \sum_{i,j=1}^{n} N_{ij}|i\rangle\langle j| = \sum_{i,j=1}^{n} |i\rangle\langle u_i|j\rangle\langle j| = \sum_{i=1}^{n} |i\rangle\langle u_i| \sum_{j=1}^{n} |j\rangle\langle j| = \sum_{i=1}^{n} |i\rangle\langle u_i|$$

where we recalled that $\sum_{j=1}^{n} |j\rangle\langle j| = I$, the identity matrix.

Summary: To go from the standard basis $|i\rangle$ to another orthonormal basis $|u_i\rangle$, we use the following unitary change of basis transformation:

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

Expressing a matrix in a different basis

Assume we are given the entries $A_{ij} = \langle i|A|j\rangle$ of some matrix $A \in \mathrm{M}_{n,n}(\mathbb{C})$. How can we express the same matrix in a different basis?

That is, how do we compute a matrix B such that $B_{ij} = \langle u_i|A|u_j\rangle$ where $\{|u_1\rangle, \dots, |u_n\rangle\}$ is some orthonormal basis?

Note that

$$B = \sum_{i,j=1}^{n} B_{ij}|i\rangle\langle j| = \sum_{i,j=1}^{n} |i\rangle\langle u_i|A|u_j\rangle\langle j| = UAU^\dagger$$

where $U = \sum_{i=1}^{n} |i\rangle\langle u_i|$ is the basis change unitary!

Summary: If U is the change of basis from $|i\rangle$ to $|u_i\rangle$ then $UAU^\dagger$ is the matrix A expressed in the new basis $|u_i\rangle$.

Pauli gates

A particularly useful set of one-qubit unitaries are the Pauli gates:

$$-\boxed{I}- \qquad -\boxed{X}- \qquad -\boxed{Y}- \qquad -\boxed{Z}-$$

- The I gate: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I|0\rangle = |0\rangle$, $I|1\rangle = |1\rangle$
- The X gate: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$
- The Y gate: $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Y|0\rangle = i|1\rangle$, $Y|1\rangle = -i|0\rangle$
- The Z gate: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

Note: Pauli matrices have lots of nice properties and are closely related to quaternions: $\{I, iZ, iY, iX\} \cong \{1, i, j, k\}$.

Third Postulate

A measurement with input dimension n, output dimension m, and outcome set S is a collection of $|S|$ matrices of size $m \times n$,

$$\{P_k : k \in S\} \subset \mathrm{M}_{m,n}(\mathbb{C})$$

known as measurement operators, that satisfy the completeness relation

$$\sum_{k \in S} P_k^\dagger P_k = I_n$$

If the system is in state $|\psi\rangle \in \mathbb{C}^n$ before the measurement, the probability of outcome $k \in S$ and the corresponding post-measurement state $|\psi_k\rangle \in \mathbb{C}^m$ is

$$p(k) = \langle\psi|P_k^\dagger P_k|\psi\rangle = \||P_k|\psi\rangle\|^2 \qquad |\psi_k\rangle = \frac{P_k|\psi\rangle}{\sqrt{\langle\psi|P_k^\dagger P_k|\psi\rangle}}$$

Probabilities of all outcomes add up to 1:

$$\sum_{k \in S} p(k) = \sum_{k \in S} \langle\psi|P_k^\dagger P_k|\psi\rangle = \langle\psi|I_n|\psi\rangle = 1$$

Orthogonal measurement

An orthogonal measurement is a measurement whose measurement operators are projectors

$$P_k = |u_k\rangle\langle u_k|$$

where $\{|u_1\rangle, \dots, |u_n\rangle\} \subset \mathbb{C}^n$ is an orthonormal basis. When measuring state $|\psi\rangle \in \mathbb{C}^n$, the probability of outcome $k \in \{1, \dots, n\}$ and the corresponding post-measurement state is

$$p(k) = |\langle u_k|\psi\rangle|^2 \qquad\qquad |\psi_k\rangle = |u_k\rangle$$

The computational or standard basis measurement corresponds to the case when $|u_k\rangle = |k\rangle$.

Example: When $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is measured in the standard basis,

$$\begin{aligned} P_0 &= |0\rangle\langle 0|, & p(0) &= |\alpha|^2 & |\psi_0\rangle &= |0\rangle \\ P_1 &= |1\rangle\langle 1|, & p(1) &= |\beta|^2 & |\psi_1\rangle &= |1\rangle \end{aligned}$$

Relative phase matters

Recall these two states from the first lecture:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad\qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

They cannot be distinguished by measuring in the computational basis since both outcomes occur with probability $1/2$.

However, these states themselves form an orthonormal basis $\{|+\rangle, |-\rangle\}$, the Hadamard basis. When measuring $|+\rangle$ in this basis, the probabilities are

$$p(+) = |\langle +|+\rangle|^2 = 1 \qquad\qquad p(-) = |\langle -|+\rangle|^2 = 0$$

so we always get the outcome "$+$". Similarly, when $|-\rangle$ is measured in this basis we always get the outcome "$-$".

While the standard basis measurement produces a uniformly random outcome and thus gives no information about which of the two states we have, the Hadamard basis measurement identifies the state perfectly!

Haidinger's brush

Source: Wikipedia

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

If the joint state of a system is $|\psi_1\rangle \otimes |\psi_2\rangle$ and the first party applies U, the new state is

$$(U \otimes I) \otimes (|\psi_1\rangle \otimes |\psi_2\rangle) = (U|\psi_1\rangle) \otimes |\psi_2\rangle$$

This is the same as the combined state of $U|\psi_1\rangle$ and $|\psi_2\rangle$.

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

Why tensor product?

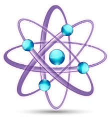
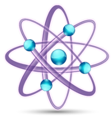
Imagine you have two random coins:

 $P = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$  $Q = \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$

What is their joint probability distribution?

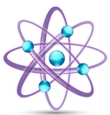
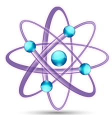
$$\begin{array}{l} 00: \\ 01: \\ 10: \\ 11: \end{array} \begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix} = \begin{pmatrix} p_0 \begin{pmatrix} q_0 \\ q_1 \end{pmatrix} \\ p_1 \begin{pmatrix} q_0 \\ q_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \otimes \begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = P \otimes Q$$

Similarly, if you have to qubit states

 $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$  $|\varphi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix}$

their joint state is $|\psi\rangle \otimes |\varphi\rangle$. Note that $\| |\psi\rangle \otimes |\varphi\rangle \| = \| |\psi\rangle \| \| |\varphi\rangle \| = 1$.

Computational basis: notation

 $|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \begin{array}{l} |0\rangle \\ |1\rangle \end{array}$  $|\varphi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \begin{array}{l} |0\rangle \\ |1\rangle \end{array}$

$$|\psi\rangle \otimes |\varphi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \beta_0 \\ \alpha_0 \beta_1 \\ \alpha_1 \beta_0 \\ \alpha_1 \beta_1 \end{pmatrix} \begin{array}{l} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array}$$

Standard basis notation for the joint system: $|i\rangle \otimes |j\rangle \equiv |i, j\rangle \equiv |ij\rangle$.
For example:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Product and entangled states

A state $|\Psi\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m$ of a combined system is product if it can be expressed as $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ for some $|\psi_1\rangle \in \mathbb{C}^n$ and $|\psi_2\rangle \in \mathbb{C}^m$. Otherwise it is called entangled.

Example: This two-qubit state is a product state:

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

Example: Neither of the following two-qubit states can be written as a product of single-qubit states, hence they are both entangled:

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Note: Physical separation does not imply that the joint state must be product! Just like two distant random coins can still be correlated, two physically separated particles can also be entangled.

How to measure only one of two qubits?

Given a state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, how do we measure only the first qubit? We tensor the desired measurement operators with I! For example, if we want to measure the first qubit in the standard basis, we take

$$P_k = |k\rangle\langle k| \otimes I = (|k\rangle \otimes I)(\langle k| \otimes I)$$

Then the probability to get outcome k is

$$p(k) = \|(\langle k| \otimes I)|\psi\rangle\|^2$$

and the post-measurement state of the two qubits is

$$|\psi_k\rangle = |k\rangle \otimes \frac{(\langle k| \otimes I)|\psi\rangle}{\|(\langle k| \otimes I)|\psi\rangle\|}$$

If we do not want to keep the first qubit around after the measurement and want to discard altogether, we can simply take $P'_k = \langle k| \otimes I$.

Summary

- **Postulate 1:** A closed system is described by a unit vector in a complex vector space.
- **Postulate 2:** The evolution of a closed system in a fixed time interval is described by a unitary transformation.
- **Postulate 3:** If a closed system is in state $|\psi\rangle$ and we measure it in an orthonormal basis $\{|u_1\rangle, \dots, |u_n\rangle\}$, we get outcome k with probability $|\langle u_k|\psi\rangle|^2$ and the system is now in the state $|u_k\rangle$.
- **Postulate 4:** The state space of a composite system is the tensor product of the state spaces of its components.

- **Expanding a state in any basis:** $|\psi\rangle = \sum_{i=1}^{n} \langle u_i|\psi\rangle |u_i\rangle$
- **Change of basis:** go from $|i\rangle$ to $|u_i\rangle$ using $U = \sum_{i=1}^{n} |i\rangle\langle u_i|$
- **Matrix in a different basis:** if A is in basis $|i\rangle$ then $UAU^\dagger$ is in $|u_i\rangle$
- **Product state:** $|\psi_1\rangle \otimes |\psi_2\rangle$
- **Entangled state:** not product, e.g., $(|00\rangle + |11\rangle)/\sqrt{2}$