Quantum Computing (CST Part II)

Lecture 3: The Postulates of Quantum Mechanics

The most incomprehensible thing about the world is that it is comprehensible.
Albert Einstein

What is quantum mechanics?

When we speak of classical mechanics we think of Newton's laws, but *quantum* mechanics is quite different – it is not a physical theory, but rather a framework for the development of physical theories.

There are four postulates of quantum mechanics that any (quantum) physical theory must satisfy.

Quantum electrodynamics (Feynman) is an example of a successful quantum physical theory, whilst a quantum theory of gravity remains elusive, and is one of the most important open problems in theoretical physics.

The four postulates of quantum mechanics

1. **State space**: how to describe a quantum state.
2. **Evolution**: how a quantum state is allowed to change with time.
3. **Measurement**: the effect on a quantum state of interaction with a classical system that yields classical information.
4. **Composition**: How to compose multiple quantum systems.

State space

Postulate 1

Associated to any isolated physical system is a complex vector space with an inner product (that is, a 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.

In this course, we consider only qubits, quantum states with space $\mathbb{C}^2$, and compositions thereof (i.e., according to postulate 4), although higher dimensional "qudit" states are sometimes considered in quantum computing literature, and indeed physically there may be infinite dimensional systems.

Examples of physical realisations of qubits:

- The spin of an electron.
- The polarisation of a photon.
- The current in a superconducting circuit.

Evolution

Postulate 2

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

$$i\hbar \frac{\mathrm{d}\,|\psi\rangle}{\mathrm{d}t} = \mathrm{H}\,|\psi\rangle$$

where $\hbar$ is the physical constant, *Planck's constant* and H is a fixed Hermitian operator known as the *Hamiltonian* of the closed system.

Evolution – simplified

In computer science, we are typically interested not in continuous time evolution, but the state at discretised time intervals. It follows that postulate 2 can thus be simplified

Postulate 2'

The change in the state of a closed quantum system from t_0 to t_1 is described by the unitary transformation:

$$|\psi_{t_1}\rangle = U\,|\psi_{t_0}\rangle$$

- This expression follows directly from the Schrödinger equation.
- The unitary operator U depends only on the underlying Hamiltonian and the times t_0 and t_1.
- In quantum computing we generally treat postulate 2' as the fundamental expression of state evolution.

The significance of unitarity

The solution to the Schrödinger equation is:

$$|\psi_{t_1}\rangle = \exp\left(\frac{-i\mathrm{H}(t_1 - t_0)}{\hbar}\right)|\psi_{t_0}\rangle$$

From which we define the unitary, U:

$$U(t_0, t_1) = \exp\left(\frac{-i\mathrm{H}(t_1 - t_0)}{\hbar}\right)$$

The unitary nature of the discrete time evolution follows directly from the Hermitian nature of the continuous time evolution, and furthermore unitary operators are the unique linear maps that preserve the norm:

$$|| \, |\psi_{t_1}\rangle \, || = ||U \, |\psi_{t_0}\rangle \, || = || \, |\psi_{t_0}\rangle \, || = 1$$

This is important, as it means that a unitary operation maps a n-qubit state to another n-qubit state.

The Pauli matrices

The Pauli matrices X, Y and Z are important one-qubit unitary matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Which has the following effect on the computational basis states,
$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$; $X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$;

$$Y = i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Which has the following effect on the computational basis states,
$Y|0\rangle = i|1\rangle$; $Y|1\rangle = -i|0\rangle$;

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Which has the following effect on the computational basis states,
$Z|0\rangle = |0\rangle$; $Z|1\rangle = -|1\rangle$.

The Hadamard matrix

Another important one-qubit unitary is the Hadamard matrix:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Which has the following effect on the computational basis states:

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \equiv |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \equiv |-\rangle$$

i.e., it puts the computational basis states in superposition. H is self-inverse, therefore:

$$H|+\rangle = |0\rangle \qquad H|-\rangle = |1\rangle$$

i.e., it interferes the superposition to recover the original computational basis states.

Unitaries applied to superpositions of basis states

As we move onto quantum computing proper, it will become increasingly natural (and important) to think of the action of unitary matrices in terms of their effect on the computational basis states.

Consider that a general one-qubit state, $|\psi\rangle$, can be expressed as a superposition (weighted sum) of the computational basis states:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

where a and b are complex in general. If we now want to express the state after some unitary, U, has been applied to $|\psi\rangle$ we get:

$$U\,|\psi\rangle = U(a\,|0\rangle + b\,|1\rangle) = aU\,|0\rangle + bU\,|1\rangle\,,$$

i.e., because of the distributivity of matrix multiplication. For example, if U is a Pauli-X operation, then:

$$X\,|\psi\rangle = X(a\,|0\rangle + b\,|1\rangle) = aX\,|0\rangle + bX\,|1\rangle = a\,|1\rangle + b\,|0\rangle$$

The same principle applies to two-qubit unitaries as well (and indeed to n-qubit unitaries for any $n \geq 1$, although our primary focus will be on one- and two-qubit unitaries in this course).

Measurement

We met measurement in an informal way in the first lecture, now we give the general measurement postulate.

Postulate 3

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 index m refers to the measurement outcomes that **may** occur in the experiment.

If the state of the quantum system is $|\psi\rangle$ directly before the measurement, the probability of the mth outcome is given by:

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

and the state of the system after the measurement is

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

Measurement (continued)

It is necessary that the probabilities of all possible outcomes sum to one, that is

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

as $|\psi\rangle$ is arbitrary and not dependent on the index m, we can see that this is satisfied by the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I$$

That is, because:

$$\begin{aligned}
\sum_m p(m) &= \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle \\
&= \langle\psi| \left(\sum_m M_m^\dagger M_m \right) |\psi\rangle \\
&= \langle\psi| I |\psi\rangle \\
&= \langle\psi|\psi\rangle \\
&= 1
\end{aligned}$$

This proves that the completeness equation is sufficient, and we can readily see that $\sum_m M_m^\dagger M_m = I$ is the only condition that achieves this for general $|\psi\rangle$, so therefore it is necessary too.

Measurement in the computational basis

In computer science, we often implicitly assume that by *measurement* we mean single qubit measurement in the computational basis. In this case, our measurement operators are

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } M_1 = |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

which we can verify satisfies the completeness equation:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}^\dagger \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}^\dagger \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Note that the measurement operators, M_0 and M_1 are projectors onto $|0\rangle$ and $|1\rangle$, respectively, and for this reason it is known as a *projective measurement*.

Now let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we have that (abusing the notation to use M_0 and M_1 to also denote the measurement *outcomes* associated with the respective measurement *operators*):

$$p(M_0) = |\alpha|^2 \qquad p(M_1) = |\beta|^2$$

which is the Born rule (you are asked to verify this in the exercise sheet).

Measurement in the $|+\rangle, |-\rangle$ basis

Consider the state $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$. If we measure this in the computational basis, we get either outcome M_0 or M_1 each with probability $1/2$. However, if we measure in the $|+\rangle, |-\rangle$ basis (recall $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$), which has measurement operators

$$M_+ = |+\rangle\langle+| = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } M_- = |-\rangle\langle-| = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

then we get state M_+ with probability 1:

$$\begin{aligned} p(M_+) &= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\ &= 1 \end{aligned}$$

Measurement in the $|+\rangle, |-\rangle$ basis (continued)

We could get the same result more quickly using Dirac notation:

$$p(M_+) = \langle +| \left(|+\rangle \langle +|\right)^\dagger \left(|+\rangle \langle +|\right) |+\rangle = \left(\langle +|+\rangle\right)^3 = 1$$

Similarly, if instead $|\psi\rangle = |-\rangle$ then we get outcome M_- with probability 1:

$$p(M_-) = \langle -| \left(|-\rangle \langle -|\right)^\dagger \left(|-\rangle \langle -|\right) |-\rangle = \left(\langle -|-\rangle\right)^3 = 1$$

Whereas if we measure in the computational basis, we still get each outcome with probability $1/2$. This is an example of the significance of relative phase.

Note that measurement in the $|+\rangle, |-\rangle$ basis is another example of a projective measurement, and in the above analysis we have implicitly used the fact that projectors are self-adjoint, i.e.,

$$\left(|\psi\rangle \langle \psi|\right)^\dagger = \langle \psi|^\dagger |\psi\rangle^\dagger = |\psi\rangle \langle \psi|$$

Global and relative phase

We can write any one-qubit state as:

$$|\psi\rangle = e^{i\theta}(\alpha\,|0\rangle + \beta e^{i\phi}\,|1\rangle) \equiv e^{i\theta}\,|\psi'\rangle$$

where α and β are positive real numbers. θ is known as the global phase, and has no observable consequences because:

$$U\,|\psi\rangle = Ue^{i\theta}(\alpha\,|0\rangle + \beta e^{i\phi}\,|1\rangle) = e^{i\theta}U(\alpha\,|0\rangle + \beta e^{i\phi}\,|1\rangle) = e^{i\theta}U\,|\psi'\rangle$$

and for any measurement operator P_m,

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

where we use the fact that $(e^{i\theta}\,|\psi'\rangle)^\dagger = \langle\psi'|\,e^{-i\theta}$ (which can easily be verified).

Thus we typically neglect global phase. The same cannot, however be said for the *relative phase*, ϕ. For example, in the previous slide $|+\rangle$ and $|-\rangle$ both have $\alpha = \beta = 1/\sqrt{2}$, but in the former $\phi = 0$, whereas in the latter $\phi = \pi$, *and we saw that measurement in the* $|+\rangle, |-\rangle$ *basis could distinguish these two* 100% *of the time.*

Composition

Postulate 4

The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

We can now see the significance of the fact that:

$$(U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle) = (U_1 |\psi_1\rangle) \otimes (U_2 |\psi_2\rangle)$$

$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ is what is known as a separable state. Let $|\psi'\rangle = (U_1 \otimes U_2)(|\psi_1\rangle \otimes |\psi_2\rangle)$, $|\psi_1'\rangle = U_1 |\psi_1\rangle$ and $|\psi_2'\rangle = U_2 |\psi_2\rangle$, we have that:

$$|\psi'\rangle = |\psi_1'\rangle \otimes |\psi_2'\rangle$$

i.e., single qubit unitary matrices applied to a separable state leads to a separable state.

Entangled states

As we shall see, quantum computing draws its advantage from the fact that not all quantum states are separable. Consider the *two qubit unitary*

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

applied to the state
$|+\rangle \otimes |0\rangle = (1/\sqrt{2}) \begin{bmatrix} 1 & 1 \end{bmatrix}^T \otimes \begin{bmatrix} 1 & 0 \end{bmatrix}^T = \begin{bmatrix} 1/\sqrt{2} & 0 & 1/\sqrt{2} & 0 \end{bmatrix}^T$:

$$\text{CNOT}(|+\rangle \otimes |0\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 1/\sqrt{2} \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}$$

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

This is an an *entangled state* which cannot be separated as tensor product. We call CNOT an *entangling* operation (or "gate" in the quantum circuit model), and even though it operates on two qubits, Postulate 2 still applies – so it is still necessarily unitary.

More on entangled states and the Bell states

In quantum computing, we take non-separability as the definition of an entangled state, and so there are infinitely many entangled states. Four important two-qubit entangled states are the Bell states:

$$
\begin{aligned}
|\Phi^+\rangle &= (1/\sqrt{2})(|00\rangle + |11\rangle) = (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix} \\
|\Phi^-\rangle &= (1/\sqrt{2})(|00\rangle - |11\rangle) = (1/\sqrt{2}) \begin{bmatrix} 1 & 0 & 0 & -1 \end{bmatrix} \\
|\Psi^+\rangle &= (1/\sqrt{2})(|01\rangle + |10\rangle) = (1/\sqrt{2}) \begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} \\
|\Psi^-\rangle &= (1/\sqrt{2})(|01\rangle - |10\rangle) = (1/\sqrt{2}) \begin{bmatrix} 0 & 1 & -1 & 0 \end{bmatrix}
\end{aligned}
$$

Which form an orthonormal basis for $\mathbb{C}^4$ (**exercise: verify this**).

What to remember

Quantum mechanics specifies four postulates to which a physical theory must adhere. You should be familiar with these, and we have also introduced the following important concepts in this lecture.

- The Pauli matrices
- The Hadamard matrix
- The significance of global and relative phase
- The existence of entangled states