Quantum Information Processing

Lecture 3

Dr. Ahmad Khonsari

Uiversity of Tehran

Fall 2022

December 16, 2022

Slides Prepared by Mahdi Dolati

What is quantum mechanics?

When we speak of classical mechanics we think of Newtons 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.

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 systems 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:

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

where $\hbar$ is the physical constant, Plancks 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 are generally treat postulate 2' as the fundamental expression of state evolution.

The significance of unitarity

The solution to the Schrödinger equation is:

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

From which we define the unitary, U:

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

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:

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

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:
$X|0\rangle = |1\rangle$; $X|1\rangle = |0\rangle$.

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

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:
$Z|0\rangle = |0\rangle$; $Z|1\rangle = -|1\rangle$.

Wolfgang Pauli

Wolfgang Pauli was a pioneer in quantum physics, notable for the Pauli exclusion principle and coining the phrase “not even wrong” (in scientific argument), amongst many other things.

Source: Wikipedia

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.

Measurement

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:

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

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

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

which we can verify satisfies the completeness equation:

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

Now let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we have that:

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

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), which has measurement operators

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

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:

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

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

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

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.

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,

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

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 $|+\rangle \otimes |0\rangle$:

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

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

an entangled state which cannot be separated as tensor product.