Lecture 2: Postulates of Quantum Mechanics

The Eigensolvers

July 6, 2021

1 Introduction

The quantum computing paradigm was first theorized in the 1980s with the quantum Turing machine by Paul Benioff. Over the last 40 years, there has been many significant breakthroughs in quantum algorithm that helps to consolidate the quantum computing model. Some of the most notable innovations includes the Shor's factoring algorithm, the Grover's search algorithm, recently the Variational Quantum Eigensolvers. These algorithms takes advantage of the unique properties of quantum systems, such as superposition, interference and entanglement, to provides non-trivial speed up to classical problems.

1.1 First postulate: Single Quantum System

In classical computations, the classical bits occupies two discrete states of 0 and 1. Logic gates acts on these bits, transforming them from one discrete states to another. In vector notations, we can represent the classical bit as a basis vector of a two level system.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

But in the quantum world, we see a new phenomenon reveal itself while tackling what values a bit can take. The properties of superposition in quantum systems allows an extension of the classical system to intermediate states between $|0\rangle$ and $|1\rangle$ i.e. it can be both $|0\rangle$ and $|1\rangle$ simultaneously. Thus we have the most fundamental unit of quantum computation, the qubit.

By the description of quantum mechanics, the qubit occupies a 2-dimensional complex Hilbert space $\mathcal{H}_1$, which is spanned by the basis vectors $|0\rangle$ and $|1\rangle$. An arbitrary qubit state $|\psi\rangle \in \mathcal{H}_1$ can be represented as a combination of the basis.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where, $\alpha, \beta \in \mathbb{C}$

The scalars α, β are called amplitudes of $|0\rangle$ and $|1\rangle$ respectively. These amplitudes affect the probability of measurements for the basis states. In our cases, when measured, the state $|\psi\rangle$ will collapse to $|0\rangle$ with probability of $|\alpha|^2$ and collapse to $|1\rangle$ with probability $|\beta|^2$.

Since the qubits can only collapse to one of the two basis states, the two probabilities add up to 1.

$$|\alpha|^2 + |\beta|^2 = 1$$

The constraint normalize the states of the qubit to a set of unit vectors, called rays. This set forms a sphere called the Bloch sphere.

1.2 Second Postulate: Quantum Operations

Quantum operators are used to evolve the qubit from one state to another. In quantum computing language, we call these quantum gates, which performs specific actions on one or more qubits within a quantum circuit. These quantum operators belongs to a special type of matrices called Unitary matrices, which preserves the norm and angles of vectors during the transformation. There a two ways to represent these transformations, as outputs to each input state or as square matrices. We represent some common quantum gates in both forms, outputs and matrices.

With single qubit gates, we have The Identity Gate (I), which performs the "do nothing" operation. As outputs, it is simply

$$I|0\rangle = |0\rangle \text{ and } I|1\rangle = |1\rangle$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

The NOT-Gate (X), which is equivalent to the classical NOT.

$$X|0\rangle = |1\rangle \text{ and } X|1\rangle = |0\rangle$$

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

The Hadamard Gate (H), which brings the basis $|0\rangle, |1\rangle$ into superposition of equal probability.

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

The Z Gate (Z), which conditionally adds a non-trivial negative phase to the qubit.

$$Z|0\rangle = |0\rangle \text{ and } Z|1\rangle = -|1\rangle$$

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

There are some more gates called the Rotation gates which are as follows

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

When quantum gates are applied to superposition states, the actions is performed independently on the basis states by linearity.

$$\begin{aligned} M|\psi\rangle &= M(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha M|0\rangle + \beta M|1\rangle \end{aligned}$$

1.3 Third Postulate: Multiple Quantum Systems

We have discussed how to represent single qubits but a quantum computer with a single qubit would not be useful. We want to represent multiple qubits together and simultaneously.
Tensor product is a operator that lets us represent two or more qubits simultaneously. Tensor product does not change the state of an individual qubit but joins two or more qubits together so it is easier to visualize, perform operations and observe them easily.
With two-qubits gates, we have tensor product gates and the non-tensor product gates.
Results of tensor products of two or more single qubit gates gives a tensor product gates. Tensor

product of two one-qubit gates gives a two qubit gate. Similarly, a three qubit gate is achieved by tensoring three one-qubit gates and so on.

$$X \otimes I = \begin{pmatrix} 0 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 1 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ 1 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 0 \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

A gate which cannot be achieved by tensoring two single-qubit gates is a non-tensor product gate. An example is the $CNOT$ gates. It cannot be describes as a tensor product of two one-qubit gates. This takes in two qubits, one control and one target.

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix}$$

The $CNOT$ gate is an example of a quantum multiplexor, which is an conditional operator whose actions depends on the values of the inputs. In circuit notation, the action of the $CNOT$ on a 2-qubits basis states defined by

$$CNOT(|q_1\rangle\,|q_0\rangle) = |q_0 \oplus q_1\rangle\,|q_0\rangle$$

The qubit q_0 is called control bit and the qubit q_1 is called the target bit.

1.3.1 Entangled States

We saw that CNOT gate cannot be represented as a tensor product of two single-qubit gates. With the same idea, there are states that cannot be expressed as a tensor product of two individual qubit states. These states demonstrate a phenomenon which is called *entanglement*

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

If a pair of qubit q_0 and q_1 is entangled, they are so tightly bound that their state cannot be represented individually, only their joint state can be described accurately. Formally, there do not exist $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^2$ such that $|\Phi^+\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. The two qubit entangled state $|\Phi^+$ is also called a *Bell State*. There are three other such bell states:

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

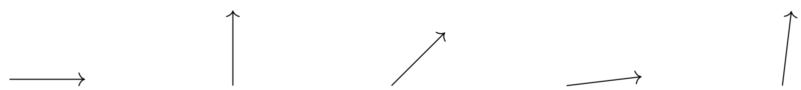
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle = \begin{pmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$

We simplified the tensor product notation from $|0\rangle|0\rangle$ to $|00\rangle$.
The four Bell States $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^+\rangle\}$ from an orthonormal basis for $\mathbb{C}^4$ also known as the *Bell Basis*

1.4 Fourth Postulate: Measurement

Classical bits can be in one of two distinct states: 0 or 1, but a single qubit can in one of infinitely many possible superposition states in between $|0\rangle$ and $|1\rangle$. Unfortunately, under the framework of quantum mechanics, it is impossible to learn what the amplitudes of a superposition are. To learn anything about a quantum state, we must make a *measurement* on the system.

A quantum mechanical measurement is akin to asking a multiple choice question about the state of the system. For example let's consider a quantum system to be an arrow in 2-dimensional space. Some possible quantum states of this arrow can be seen in Figure 1. One possible measurement on this system would be to measure whether the arrow is horizontal or vertical.



(a) (b) (c) (d) (e)

Figure 1: Possible states for our quantum arrow.

Clearly, state (a) is horizontal and state (b) is vertical, but what about the rest? The question "Is the arrow horizontal or vertical?" is only meaningful for these states. The other states are superpositions of horizontal and vertical arrows, they don't have an answer to this question. But just by looking at them, you can see that (d) is clearly more horizontal than vertical, (e) is clearly more vertical than horizontal and (c) is right in the middle of horizontal and vertical. A quantum mechanical measurement forces the state to change, or *collapse*, into either (a) or (b) because only those states can meaningfully answer the question.

Arrows (c), (d) and (e) are superpositions of (a) and (b), the probability that the measurement will collapse the state into (a) is equal to the square of the absolute value of the amplitude of (a) in the superposition. This means that (c) is equally likely to be measured as either horizontal or vertical, (d) is more likely to be measured as horizontal than vertical, (e) is more likely to be measured as vertical than horizontal, (a) will always be measured as horizontal and (b) will always be measured as vertical. Let us formalize this notion for qubits now.

A projective measurement in the basis $\{|a\rangle, |b\rangle\}$ collapses a qubit that was initially in the state $|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$ into the state $|a\rangle$ with probability

$$\Pr(a) = |\alpha|^2$$

or collapses it into the state $|b\rangle$ with probability

$$\Pr(b) = |\beta|^2$$

. Upon doing the measurement, we will learn the outcome of the measurement as either $|a\rangle$ or $|b\rangle$.

In the context of quantum computing, we will usually only consider measurements that are done in the $\{|0\rangle, |1\rangle\}$ basis, but we are free to choose any orthonormal basis to measure in.