TS70006 : Quantum Information and Quantum Computation **Spring 2019**

Lecture 1: January 16, 2019

Lecturer: Arpita Maitra *Scribes: Arpita Maitra*

1.1 Introduction

The basic model of classical computers have been visualized by Alan Turing, Von Neumann and several other researchers in 1930's and the decade after that. The technological development in the next eighty years brought us to an era where we can easily afford a small hand-held device that can compute more than $10^9 \approx 2^{30}$ operations in a second. Further, most of the communications (even secure ones over the public channel) in the world can be executed in less than a second through the internet based systems. The society, at large, is at the mercy of computing and communication technology.

However the model of computers, that Turing or Neumann thought, are limited by classical physics and those are usually known as classical computers. Till the end of nineteenth century, the physicists believed that Newtonian laws governing the motion of material bodies and Maxwells theory of electromagnetism are the most fundamental areas of physics. However, the discovery of X-rays and electrons towards the end of this century ultimately helped the scientists to comprehend quantum mechanics around 1925.

In 1982, Richard Feynman proposed the seminal idea of a universal quantum simulator or more informally, a quantum computer. Roughly speaking, a quantum system of more than one particles can be described by a Hilbert space whose dimension is exponentially large in the number of particles. Thus, it is expected that a quantum system can efficiently solve a problem that may require exponential time on a classical computer. During 1980s, the works by Deutsch-Jozsa and Grover could explain quantum algorithms that are exponentially faster than the classical ones. Most importantly, in 1994, Shor pointed out that in quantum paradigm, factorization and discrete log problems can be efficiently solved that had a major impact in classical cryptography.

The fundamental element of quantum information theory is a qubit. In this elementary lecture we are trying to understand what is a qubit? How can we recognize a qubit physically? What is Bloch sphere representation of a qubit? We will also discuss some basic algebra of qubits and quantum gates.

1.2 Basics of a Qubit

1.2.1 Qubits in Bra-Ket notation

We are familiar with classical bits 0 and 1. The quantum counter-parts of these 0 and 1 are $|0\rangle$ and $|1\rangle$ respectively. The formal nomenclature for the symbols $|\rangle$ and $\langle|$ are *ket* and *bra* respectively. $|\rangle$

symbol represents a column vector of a Hilbert space whereas $\langle|$ symbol represents a row vector of the Hilbert space. These symbols were introduced by the famous physicist Paul Dirac in 1939.

A qubit exhibits a unique property. Any qubit can be represented as a superposition of other two qubits. For example, we learned that $|0\rangle$ and $|1\rangle$ are two distinct qubits. However, $\alpha|0\rangle + \beta|1\rangle$ is also a qubit, where $\alpha, \beta \in \mathbb{C}$ (i.e., complex numbers) and $|\alpha|^2 + |\beta|^2 = 1$.

Exercise: Express the above qubit as the superposition of $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

A qubit can be physically realized by one degree of freedoms of either an electron (fermion) or a photon (boson). For example, if we consider Z-direction spin of an electron, then "Up" spin means $|0\rangle$, "down" spin means $|1\rangle$ (Here, we assume that the students are familiar with the spin quantization of electron).

If we consider Fock state, i.e., the value inside the ket represents the number of photons present in one quanta, then $|0\rangle$ means absence of photon whereas $|1\rangle$ implies the presence of single photon.

If we consider polarization of a photon, then $|0\rangle$ represents "Horizontal" polarization whereas $|1\rangle$ stands for "Vertical" polarization.

If we consider time of arrival of a photon in some port, then early arrival is represented by $|0\rangle$ whereas late arrival of a photon is represented by $|1\rangle$. We can summarized these by a table.

Physical support	Name	Information support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photon	Fock state	Vacuum	Single photon state
	Time bin encoding	Time of arrival	Early	Late
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron

The vector representation of $|0\rangle$ is $\begin{pmatrix}1\\0\end{pmatrix}$. And the vector representation of $|1\rangle$ is $\begin{pmatrix}0\\1\end{pmatrix}$.

So, the vector representation of a general qubit as a superposition of $|0\rangle$ and $|1\rangle$ is $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$.

1.2.2 Some examples of qubits

: We know that being a valid qubit we have to satisfy the following equation, i.e.,

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

So, followings are the valid examples of some qubits.

$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1+i}{2}\left|1\right\rangle$$
$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1-i}{2}\left|1\right\rangle$$
$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle$$

Exercise: Find the solution for β, if $\alpha = \frac{1}{\sqrt{2}}$ for a qubit of the form $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$.

1.2.3 Bloch Sphere Representation

Next we present a geometrical interpretation of a qubit, where a qubit is considered to be a point on a unit sphere called Bloch sphere. Consider, a qubit $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$. Since α and β are complex, assume $\alpha = r_1 e^{i\gamma}$, $\beta = r_2 e^{i(\gamma+\phi)}$. Then $|\alpha| = r_1$, $|\beta| = r_2$. Let $r_1 = \cos\theta$, $r_2 = \sin\theta$. Hence, $\alpha = \cos\theta e^{i\gamma}$, $\beta = \sin\theta e^{i(\gamma+\phi)}$, where θ, ϕ and γ are real. Thus, any qubit $\left|\phi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ can be written as $e^{i\gamma}(\cos\theta\left|0\right\rangle + e^{i\phi}\sin\theta\left|1\right\rangle)$. Further, two qubits $e^{i\gamma}(\cos\theta\left|0\right\rangle + e^{i\phi}\sin\theta\left|1\right\rangle)$ and $(\cos\theta\left|0\right\rangle + e^{i\phi}\sin\theta\left|1\right\rangle)$ are treated on equal footing under measurement, since they differ only by an overall phase factor which has no observable effect. The qubit $(\cos\theta\left|0\right\rangle + e^{i\phi}\sin\theta\left|1\right\rangle)$ is mapped to a point $(1, \theta, \phi)$ on the unit Bloch sphere. Here θ and ϕ are the usual polar and azimuthal angles respectively, and they are related to the Cartesian coordinates (x, y, z) through the usual relations $x = \cos\phi\sin\theta$, $y = \sin\phi\sin\theta$, $z = \cos\theta$. Hence, it is clear that infinite number of qubits are mapped into a single point on the Bloch Sphere.

If we fix $\phi = 0$, then we obtain states of the form $\cos\theta\left|0\right\rangle + \sin\theta\left|1\right\rangle$ and $\cos\theta\left|1\right\rangle - \sin\theta\left|0\right\rangle$ for $0 \leq \theta \leq \pi$. These lie on the polar great circle of the Bloch sphere. On the other hand, for $\theta = \frac{\pi}{4}$, one obtains states of the form $\frac{1}{\sqrt{2}}(\left|0\right\rangle + e^{i\phi}\left|1\right\rangle)$ and $\frac{1}{\sqrt{2}}(\left|0\right\rangle - e^{i\phi}\left|1\right\rangle)$ for $0 \leq \phi \leq 2\pi$ which lie on the equatorial great circle.

1.2.4 Basic Algebra

The basic algebra relating to more than one qubits is as follows that can be interpreted as tensor products. We have the classical bits as $0, 1$ and the quantum counterparts are $|0\rangle, |1\rangle$. The qubit $|0\rangle$ can be written as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle$ can be written as $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. The superposition of $|0\rangle, |1\rangle$, i.e., $\alpha|0\rangle + \beta|1\rangle$ can be written as $\alpha\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. Now consider tensor product of two qubits as $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$

$$= \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}$$

$$= \begin{bmatrix} \alpha_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \\ \beta_1 \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{bmatrix}$$

$= \alpha_1\alpha_2 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha_1\beta_2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta_1\alpha_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \beta_1\beta_2 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$

$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$. That is,

$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$.

However, any 2-qubit state may not be decomposed as above. Consider the state $\gamma_1|00\rangle + \gamma_2|11\rangle$ with $\gamma_1 \neq 0, \gamma_2 \neq 0$. This cannot be written as $(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$). This phenomenon is described as entanglement. An example of maximally entangled state is $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, which is an example of Bell states or EPR pairs. To be specific the Bell states are $\frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$ and $\frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$,

1.2.5 Quantum gates

All quantum gates are quantum mechanical operators. Quantum mechanical operators are Hermitian, i.e., there exists an inverse corresponding to all the operators. Hence, quantum gates can be considered as a reversible circuit having n qubit inputs and n qubits outputs. Mathematically, they can be seen as $2^n \times 2^n$ unitary matrices where the elements are complex numbers. Let us first present a few examples of single input single output quantum gates.

Quantum input	Quantum gate	Quantum Output
$\alpha|0\rangle + \beta|1\rangle$	X	$\beta|0\rangle + \alpha|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$	Z	$\alpha|0\rangle - \beta|1\rangle$
$\alpha|0\rangle + \beta|1\rangle$	H	$\alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

In matrix form, the gate operations are as follows:

the X gate: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$;

the Z gate: $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix}$;

the H gate: $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{\alpha+\beta}{\sqrt{2}} \\ \frac{\alpha-\beta}{\sqrt{2}} \end{bmatrix}$.

Note that $\frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle = \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

The 2-input 2-output quantum gates can be seen as 4×4 unitary matrices. An example is the CNOT gate which works as follows: $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$, $|11\rangle \to |10\rangle$. The related matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

As an application of these gates, let us describe the following circuit to create entangled state. Note that, $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, $|\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$, $|\beta_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$, and $|\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

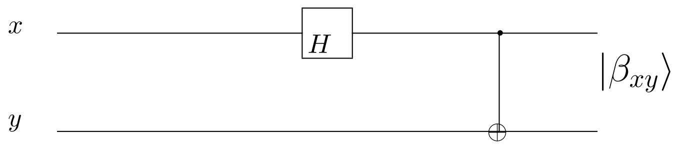

Figure 1.1: Quantum circuit for creating entangled state

Another 2-input 2-output gate is Swap gate. It swaps the states. Explicitly, let $|a\rangle$ is put in port A and $|b\rangle$ is in port B. Then after swapping, $|b\rangle$ is switched to port A and $|a\rangle$ is switched to port B. If $|a\rangle$ and $|b\rangle$ are computational basis states, then the gate works as follows $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow |10\rangle$, $|10\rangle \rightarrow |01\rangle$, $|11\rangle \rightarrow |11\rangle$. The related matrix is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Excersize: Write the matrix and draw a circuit with Hadamard and Cnot gates for the following gate operation; $|00\rangle \rightarrow |00\rangle$, $|01\rangle \rightarrow \frac{1}{\sqrt{2}}|01+10\rangle$, $|10\rangle \rightarrow \frac{1}{\sqrt{2}}|01-10\rangle$, $|11\rangle \rightarrow |11\rangle$.

1.2.6 Facts To Remember for Quantum Circuits

When dealing with quantum circuits, we have to remember the following things.

- "loops" or feedback from one part of the quantum circuit to another is not allowed. The circuit is called "acyclic"[Ref. Nielsen and Chuang, Quantum Computation and Quantum Information].
- Classical circuit allows "FANIN", i.e., in classical circuit wires can be joined together. The input of the resulting single wire is considered as the bitwise OR of all the inputs of the wires joined together. As bitwise OR operation is not reversible and hence not unitary, we can not allow "FANIN" in our quantum circuit.
- "FANOUT" where several copies of a bit are produced is also not allowed in quantum circuits due to No Cloning Theorem. We will see an example of this in the next class when we attempt to design a circuit to copy a qubit.