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

Lecture 2: January 18, 2019

Lecturer: Arpita Maitra *Scribes: Arpita Maitra*

2.1 Introduction

In the last lecture, we have discussed quantum gates which are actually quantum mechanical operators. The necessary condition to be a quantum gate is that it must be reversible. That is if outputs of the gate are considered as inputs, then we get back the actual inputs. For example, consider Hadamard gate. Hadamard gate when operated on $|0\rangle$, creates equal superposition of $|0\rangle$ and $|1\rangle$. Here, $|0\rangle$ is the input and $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ is output. Now, swap the place of input and output, i.e., consider $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ as input. We will observe that after Hadamard operation, we get back $|0\rangle$. However, in classical domain all the gates might not be reversible. For example, 'AND', 'OR', 'NAND', 'NOR' etc. gates are not reversible. Whereas classical 'NOT' gate is reversible. We can make any classical gate reversible. We will discuss that later in today's lecture. Before that we will discuss more about quantum gates.

2.2 Quantum gates

2.2.1 Single qubit gates

In last class we leaned about X gate, Z gate, Y gate and H gate. There are two more single qubit gates which play important role in quantum information. Those are S gate and T gate. T gate is also called "$\pi/8$" gate. Matrix representation of these gates are as follows.

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(\frac{i\pi}{4}) \end{pmatrix}$$

You may wonder why we would call T gate as $\pi/8$ gate when the matrix element contains $\pi/4$. Notice that we can manipulate the matrix as follows.

$$\begin{aligned} T &= \begin{pmatrix} 1 & 0 \\ 0 & \exp(\frac{i\pi}{4}) \end{pmatrix} \\ &= \exp\left(\frac{i\pi}{8}\right) \begin{pmatrix} \exp(\frac{-i\pi}{8}) & 0 \\ 0 & \exp(\frac{i\pi}{8}) \end{pmatrix} \end{aligned}$$

That is why T gate is often referred as "$\pi/8$" gate.

2.2.2 Universal set of gates

In classical domain, there exist a small set of gates exploiting which one can compute an arbitrary classical function. We say that such a set of gates is *universal* for classical computation. For example, consider the set containing AND, OR and NOT gates. Now, let we want to construct XOR gate. The corresponding truth table for XOR operation is as follows considering a and b as inputs.

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

This truth table can be obtained exploiting the following circuits.
draw the circuit here.
Similarly, in quantum domain there exist some universal set of gates. The only difference is that in classical domain we can construct the exact function according to our need from AND, OR and NOT gates whereas in quantum domain, any unitary operation may be approximated to arbitrary accuracy by a quantum circuit involving only those gates.

It can be shown that an arbitrary unitary operator may be expressed exactly as a product of two qubit unitary operators. Again, any arbitrary two qubit operator can be expressed exactly using single qubit and Cnot gates. Interestingly, any single qubit operation may be approximated to an arbitrary accuracy using the Hadamard, S, and T gates. This in turn implies that any unitary operation can be approximated to an arbitrary accuracy using Hadamard, S, T and Cnot gates. For proof, please consult Nielsen and Chaung, Quantum Computing and Quantum Information, Chap 4, Quantum Circuits.

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

2.2.3 Swap gate

Swap gate is 2-input 2-output 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: Construct the circuit for Swap operation with three CNOT gates.

2.2.4 Control U gate

"If A is true, then do B" –this type of controlled operation has enormous importance in classical as well as quantum computation. Now, we are going to explain how complex controlled operations can be implemented using quantum circuits built from elementary operations.

In the last class, we have discussed Controlled Not gate; in short Cnot gate. The matrix representation of Cnot gate is

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

Now, divide the matrix into four 2×2 sub-matrices, i.e., the above matrix now can be written as

$$\begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}.$$

Note that $A_4 = X$ gate. That is why Cnot gate is called Controlled X gate or C_x gate.

Now, let U is an arbitrary single qubit gate. Any two qubit controlled U gate can be represented by a matrix of the above form where A_4 corresponds to the U gate. Now, we can easily form the matrix for Controlled Z gate. That is

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

Any arbitrary two qubit controlled U gate is

$$Controlled - U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{bmatrix}.$$

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 $|\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$.

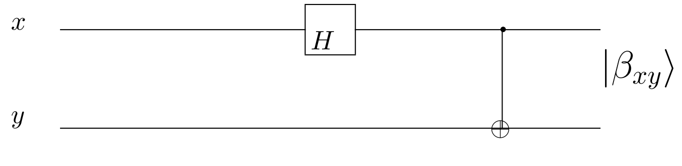


Figure 2.1: Quantum circuit for creating entangled state

2.2.5 Three qubits controlled gate

In last class we mention about Toffoli gate which is a 3-input 3-output gate. Toffoli gate can be visualized as Controlled-Cnot gate. Matrix representation of Toffoli gate is as follows.

$$C_{cnot} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Note that, here, A_1, A_2, A_3 and A_4 are 4×4 matrices and A_4 =Cnot gate. Toffoli can be also viewed as Controlled- Controlled-Not gate. Notice that all the 2×2 diagonal block matrices are identity matrix except the last diagonal block matrix. It is the matrix of X-gate.

So, the general trick of writing an arbitrary $2^n \times 2^n$ Controlled-$\cdots$-Controlled-U is as follows, where U is a $2^m \times 2^m$ matrix; $m < n$.

- Divide the whole matrix into $2^m \times 2^m$ sub-matrices. The number of block diagonal $2^m \times 2^m$ matrices should be $k = 2^{n-m}$.
- Choose $k - 1$ upper diagonal matrices. All these matrices should be $2^m \times 2^m$ Identity matrix.
- Consider the last remaining diagonal $2^m \times 2^m$ block matrix. That should be U.
- All other off-diagonal matrices should be $2^m \times 2^m$ Null matrix.

For example, consider Fredkin gate. This is also a 3 input-3 output gate. Fredkin gate can be visualized as Controlled-Swap gate. The matrix representation is then

$$C_{swap} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2.2.6 No cloning Theorem

In classical paradigm, we can copy a bit. However, in quantum domain, if we do not know the values of α and β, perfect cloning is not possible for a qubit, $\alpha|0\rangle + \beta|1\rangle$. The proof is as follows.

Let there exist a unitary operator U which does the copying procedure. Mathematically it can be written as $U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$. Remind that U is a unitary operator, i.e., $UU^\dagger = I$. $((U^\dagger)_{ij} = \overline{U}_{ji}$, transpose and scalar complex conjugate.) Let this copying procedure works for two particular pure states, $|\psi\rangle$ and $|\phi\rangle$. Then we have

$$U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle, U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$$

Now, take the inner product of these two, i.e., $\langle s|\langle\psi|U^\dagger U|\phi\rangle|s\rangle = \langle\psi|\langle\psi||\phi\rangle|\phi\rangle$. This implies $\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2$. This is equivalent to the following equation.

$$x = x^2$$

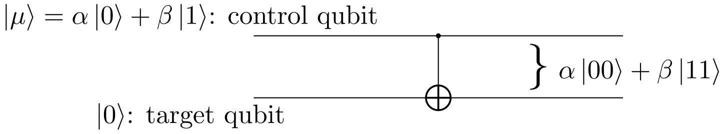
. This equation has only two solutions.

- $x = 0$ and
- $x = 1$.

Thus we get either $|\psi\rangle = |\phi\rangle$ or the inner product of them equals to zero, i.e., $|\psi\rangle$ and $|\phi\rangle$ are orthogonal to each other.

Hence, a cloning device can only clone orthogonal states. Therefore a general quantum cloning device is impossible.

Now, we see if we can clone a qubit $|\mu\rangle$ using Cnot gate. Following is the circuit for creating a copy of $|\mu\rangle$.


$|\mu\rangle = \alpha|0\rangle + \beta|1\rangle$: control qubit
$\} \ \alpha|00\rangle + \beta|11\rangle$
$|0\rangle$: target qubit

Set $\beta = 0$; we get exact copy of control qubit. Similarly, set $\alpha = 0$, we get exact copy of control qubit. However, for $\alpha, \beta \neq 0$, we never get an exact copy of the control qubit, unless we know the values of α and β.

2.2.7 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.

2.2.8 Reversible circuits

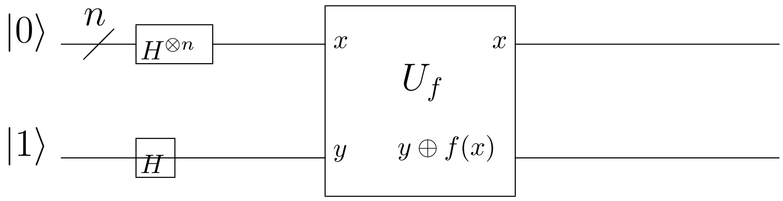
We leant that classical gates are not necessarily reversible as a classical gate defines a function f from some input bits $\{0,1\}^n$ to some output bits $\{0,1\}^m$. If this function is a bijection, then we say that this circuit is reversible. Recall that a bijection means that for every input to the function there is a single unique output and for every output to the function there is a single unique input. Thus given the output of a reversible function, we can uniquely construct its input. A gate which is not reversible is called irreversible. Note that our definition of reversible requires $n = m$.

In classical domain, one may convert an irreversible gate to a reversible gate by adding some extra input bits which are called "garbage" bits. Let $x = x_0, x_1, x_2, \cdots x_{n-1}$ are some actual input bits. We add one wire for an extra bit y. The functionality of this new gate is now defined as

$$F(x, y) = (x, y \oplus f(x))$$

where, $f(x)$ is the functionality of the irreversible gate considered.

Now, take the outputs, i.e., $(x, y \oplus f(x))$ as the inputs. At the output ports we will get $(x, y \oplus f(x) \oplus f(x)) = (x, y)$. This idea is exploited in quantum domain to construct a unitary gate for an arbitrary Boolean function $f(x)$. The following circuit shows how one can construct a unitary quantum gate for an arbitrary Boolean function $f(x)$.


|0⟩
n
H^{⊗n}
|1⟩
H
x
x
U_f
y
y ⊕ f(x)