Week 2 : Gate Model of Computation

Contents

1 Quantum Gates

Quantum gates like their classical counterparts, perform operations on their input and convert it into an output. Recall that quantum states are always normalized such that for any quantum state $\sum_j \alpha_j |\psi\rangle_j$ with amplitudes $\{\alpha_j\}$, we have $\sum_j \alpha_j^2 = 1$. Hence the quantum input states need to be normalized, and the quantum gates give normalized output states.
The actual place where the two models fundamentally differ is that the quantum gates always perform reversible operations. This property of quantum gates has its roots in quantum mechanics, which mandates that all quantum operators are unitary. This means that we can have a matrix representation for all quantum operations (or gates), and these matrices have to be unitary, i.e.

$$UU^\dagger = I$$

where we obtain $U^\dagger$ by transposing and then complex conjugating U. Now we begin by looking at some common quantum gates.

1.1 The Hadamard Gate

The Hadamard Gate is a single qubit gate represented by the matrix

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

Let us its effects on the basis states $|0\rangle$ and $|1\rangle$.

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right) \\ H|1\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right) \end{aligned} \tag{2}$$

In equation 2, we see that in both cases, the Hadamard gate gives an output that has an equal chance of collapsing to either of the basis states. Hence the Hadamard gate creates a superposition!
Exercise: Verify for yourself that the Hadamard gate is unitary.

1.2 The Pauli gates

The Pauli-X gate is a single qubit gate that flips the amplitude of the qubit. Hence it is also known as the Quantum analogue of the NOT gate. Pauli-X (σ_X) is represented by the matrix

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3}$$

Let us its effects on the basis states $|0\rangle$ and $|1\rangle$.

$$\begin{aligned} \sigma_X|0\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ \sigma_X|1\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{aligned} \tag{4}$$

Exercise: Verify for yourselves that σ_X is unitary.
The Pauli-Y gate is represented as

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{5}$$

The Pauli-Y gate is represented as

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{6}$$

The Pauli-Z gate is represented as

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{7}$$

We can see that σ_Z flips the phase of the basis state $|1\rangle$, but leaves $|0\rangle$ unchanged.
Exercise: Verify for yourselves that the Pauli gates are unitary and involutary[1].

1.3 The Phase Shift Gates

This is a family of single-qubit gates that leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$. They are represented as

$$\mathbf{R}_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \tag{8}$$

The probability of measuring the basis states is unchanged after applying this gate as it just modifies the phase of the quantum state. The Pauli-Z gate is just a special case the the Phase Shift Gates.

1.4 The C-NOT gate

This is our first 2-qubit gate. It is represented by

$$\begin{bmatrix} I & 0_{2\times 2} \\ 0_{2\times 2} & \sigma_X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{9}$$

The first qubit acts as the control, and C-NOT performs the NOT operation on the second qubit only if the first qubit is 1. Basically for $a, b \in \{0, 1\}$, $|a, b\rangle \xrightarrow{\text{C-NOT}} |a, a \oplus b\rangle$.
Exercise: Create the controlled version of the gates for σ_Y and verify that it is unitary. There are a lot of other quantum gates, namely the SWAP gate for 2 qubits and the C-SWAP, Toffoli and Fredkin gates for 3 qubits. The reader is encouraged to look up these gates on their own time as they will be used later on in this lecture series.

2 Quantum Wires

A quantum wire is a wire in a quantum circuit. Unlike its classical counterpart, quantum wires need not be actual wires (that conduct electricity). Instead quantum wires can also be thought of as the passage of time, or passage of space.
One important distinction between classical wires and quantum wires is that there is no *FAN-IN* operation (multiple wires are merged together into a single wire) or *FAN-OUT* operation (several copies of a bit on an input wire are produced). *FAN-IN* occurs through a bitwise-OR of the input wires and is an irreversible operation, hence not unitary. *FAN-OUT* is forbidden because of the **No-Cloning Theorem**, which states that it is impossible for any quantum circuit to make copies of an arbitrary quantum state. We shall study this later in detail.

3 Quantum Circuit

Quantum Circuits are a sequence of quantum gates connected by quantum wires. The physical realization of a quantum algorithm translates to a quantum circuit. Hence quantum circuits are a model of quantum computation.

[1] A is an involutary matrix if $A^2 = I$

4 Quantum Entanglement

Postulate 4, from last week's lecture material, allows us to define a concept most fundamental to quantum computation – entanglement. Consider,

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

This state has a remarkable property that their exist no single qubit states $|a\rangle$ and $|b\rangle$ such that $|\psi\rangle = |a\rangle\,|b\rangle$. The reader is encouraged to prove this an exercise (hint: consider $|a\rangle = \alpha_a\,|0\rangle + \beta_a\,|1\rangle$ and $|b\rangle = \alpha_b\,|0\rangle + \beta_b\,|1\rangle$). Any composite system having this property is an *entangled* state.

5 Creating an Entanglement

Entangled states play a very important role in quantum computing and quantum information as we will see in the coming weeks. It is only natural for us to ask how create a pair of entangled qubits. The Hadamard and C-NOT gates that we have studied about will help us make the circuit shown in Figure 1. The reader

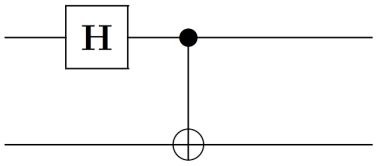

Figure 1: Quantum circuit for entangling two qubits (Credits: John Preskill's lecture notes)

is asked to verify that we get the following outputs for the given inputs:

$$|00\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle \to \left|\varphi^+\right\rangle$$
$$|01\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|1\rangle \to \left|\psi^+\right\rangle$$
$$|10\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|0\rangle \to \left|\varphi^-\right\rangle$$
$$|11\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|1\rangle \to \left|\psi^-\right\rangle$$

These output states are called the Bell states or EPR pairs.

6 No Cloning Theorem

Theorem 1. *There exists no unitary operator U such that for any arbitrary quantum state $|\psi\rangle$ and a random ancilla $|\phi\rangle$, we can perform the following transformation*

$$|\psi\rangle \otimes |\phi\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \tag{10}$$

Proof. We show a proof of Theorem 1 by contradiction. Suppose we can perform the transformation shown in equation 10, and let there be two arbitrary quantum states $|\psi\rangle$ and $|\Psi\rangle$. Then for an appropriate U we would have

$$U|\psi\rangle \otimes |\phi\rangle = e^{i\alpha}|\psi\rangle \otimes |\psi\rangle \tag{11}$$
$$U|\Psi\rangle \otimes |\phi\rangle = e^{i\beta}|\Psi\rangle \otimes |\Psi\rangle \tag{12}$$

where α and β are the phases. Now we take the Hermitian conjugate of (12).

$$\langle\Psi| \otimes \langle\phi|U^\dagger = e^{-i\beta}\langle\Psi| \otimes \langle\Psi| \tag{13}$$

Now multiplying (11) and (13) together we get

$$\begin{gathered}\langle\Psi| \otimes \langle\phi|U^\dagger U|\psi\rangle \otimes |\phi\rangle = e^{-i\beta}\langle\Psi| \otimes \langle\Psi|e^{i\alpha}|\psi\rangle \otimes |\psi\rangle \\ \langle\Psi|\psi\rangle \otimes \langle\phi|\phi\rangle = e^{i(\alpha-\beta)}\langle\Psi|\psi\rangle \otimes \langle\Psi|\psi\rangle \\ \text{Taking absolute value on both sides we get} \\ |\langle\Psi|\psi\rangle| = |\langle\Psi|\psi\rangle|^2\end{gathered} \tag{14}$$

The solution to equation 14 is

$$|\langle\Psi|\psi\rangle| = \begin{cases} 1, & \text{If } \langle\Psi| \text{ and } |\psi\rangle \text{ only have a phase difference} \\ 0, & \text{If } \langle\Psi| \text{ and } |\psi\rangle \text{ are orthogonal} \end{cases} \tag{15}$$

However we initially started out with the assumption that both $|\psi\rangle$ and $|\Psi\rangle$ are two arbitrary quantum states. Therefore there cannot exist a unitary U that can clone any arbitrary quantum state. □

7 Super Dense Coding

Let Alice and Bob be two friends very far away from each other. Now suppose Alice wants to send two bits of information to Bob. Classically, she has to send two bits via some classical communication channel. But through a quantum channel, she can send the information of two bits using just a single qubit given that Alice and Bob have an EPR pair shared between them apriori. Super dense coding helps us achieve that. The circuit for implementing super dense coding is presented in Figure 2

Let the two bits of information that Alice wants to send Bob be $b_1 b_2$. The circuit starts with an entangled pair. Alice first applies a controlled-NOT controlled on the bit b_2 and a controlled-Z controlled on the bit b_1. The evolution of the state of the system after these operations is as

$$\begin{aligned}\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &\xrightarrow{cX\otimes I} \frac{1}{\sqrt{2}}(|b_2\rangle\,|0\rangle + |\overline{b_2}\rangle\,|1\rangle) \\ &\xrightarrow{cZ\otimes I} \frac{1}{\sqrt{2}}\big((-1)^{b_1\cdot b_2}\,|b_2\rangle\,|0\rangle + (-1)^{b_1\cdot\overline{b_2}}\,|\overline{b_2}\rangle\,|1\rangle\big)\end{aligned}$$

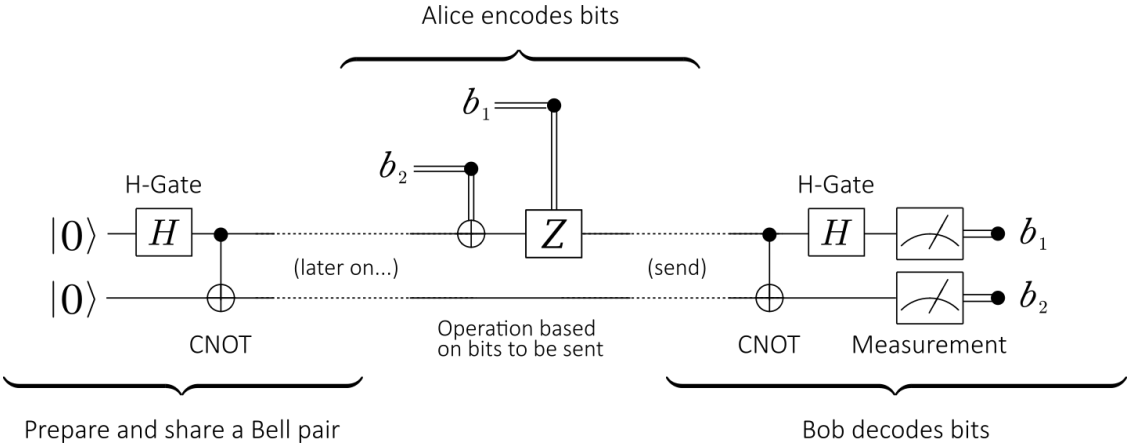

Figure 2: Quantum circuit for super dense coding (Credits: quantum-bits.org)

After these operations, Alice sends the first qubit to Bob through a quantum channel. After Bob receives the first qubit, he applies a controlled-NOT on second qubit controlled on the first and then a hadamard on

the first. The evolution of the system under these operations are given as

$$\frac{1}{\sqrt{2}}\left((-1)^{b_1\cdot b_2}\left|b_2\right\rangle\left|0\right\rangle+(-1)^{b_1\cdot\overline{b_2}}\left|\overline{b_2}\right\rangle\left|1\right\rangle\right)\xrightarrow{cX_{1,2}}\frac{1}{\sqrt{2}}\left[(-1)^{b_1\cdot b_2}\left|b_2\right\rangle+(-1)^{b_1\cdot\overline{b_2}}\left|\overline{b_2}\right\rangle\right]\left|b_2\right\rangle$$
$$\xrightarrow{H\otimes I}\left|b_1\right\rangle\left|b_2\right\rangle$$

On measuring the two qubits, Bob obtains the two bits of information $b_1 b_2$.

8 Quantum Teleportation

Imagine the following scenario. Suppose Alice has a qubit which she wished to send to Bob. But she does not know the state of the qubit and she has only a classical communication channel. Quantum teleportation will help Alice to send the exact state of the qubit to Bob by sending just two bits of information to Bob given that Alice and Bob initially share an EPR pair. The teleportation is executed using the circuit in Figure 3.

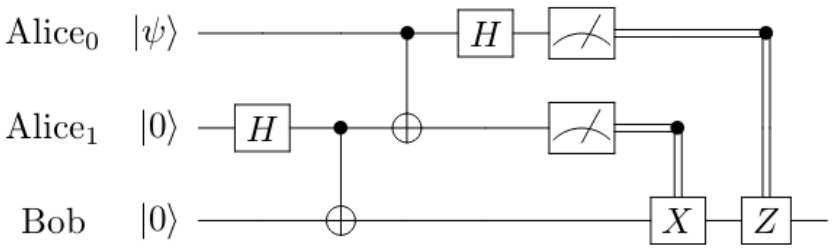

Figure 3: Quantum circuit for teleportation

Alice essentially measures the qubit to be sent and her entangled qubit in Bell basis and sends the output to Bob. Bob on receiving the two bits of information, depending on the state of the received bits, applies one of the following operations:

$$00 \longrightarrow I,\ 01 \longrightarrow X,\ 10 \longrightarrow Z,\ 11 \longrightarrow XZ$$

On performing the above operation, Bob obtains the state $|\psi\rangle$ in his qubit. One can misthink that the state $|\psi\rangle$ is being copied to Bob's qubit. However, notice that the state $|\psi\rangle$ possessed by Alice gets destroyed when Alice measures it. So at any particular time, there is at most one qubit of state $|\psi\rangle$ and so there is no violation of no cloning theorem.

Quantum teleportation is a tool that illustrates the power of quantum entanglement. It is a very powerful tool to transfer information from one location to another with just a classical channel and pre-shared entangled qubits. So quantum teleportation is an important resource for quantum communication.

9 Exercises

1. The right and left basis states of a single qubit system is defined as

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

   Give the matrix of the gate (a unitary transformation) that transforms (i)the computational basis states (i.e, the states $|0\rangle, |1\rangle$), (ii)the Hadamard basis states (i.e, the states $|+\rangle, |-\rangle$) into right and left basis states.

2. Show the following equivalences:

   (a) HXH = Z

   (b) HYH = -Y

   (c) HZH = X

3. A CNOT gate is implemented on two qubits, the first qubit being the control, the second qubit is the target. We denote this by $CNOT_{1,2}$. Show that applying H gate on both the qubits before and after the $CNOT$ performs the operation $CNOT_{2,1}$.

4. We know that a $CNOT$ gates acts as $CNOT\,|a\rangle\,|b\rangle \longrightarrow |a\rangle\,|b \oplus a\rangle$. So after a $CNOT$, the target qubit also contains information about the control qubit. Construct a circuit C, just using $CNOT$ gates that just swaps the qubit., i.e, $C\,|a\rangle\,|b\rangle \longrightarrow |b\rangle\,|a\rangle$.

5. A Toffoli gate is a gate implemented on 3 qubits, the first two qubits are the control qubits and the last qubit is the target qubit. On implementing the Toffoli gate, the control qubit is flipped if the control qubits are set to 1. Is it possible to construct a Toffoli gate just by using CNOT gates? If yes, contruct a circuit only using CNOT gates that implement a Toffoli gate and if no, justify why.

6. A multi-control Toffoli gate is a gate that flips the target qubit if all the qubits control qubits are set to 1 and the number of qubits can be arbitrarily set. Construct a quantum circuit that implements a 5-control Toffoli gate by using only Toffoli gates. (Feel free to use some ancilla qubits if necessary).

7. Give a step by step evolution of the states during a quantum teleportation protocol where Alice tries to send the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ to Bob.