Lecture 3 - Sharing Quantum States

The Eigensolvers

July 7, 2021

1 Introduction

In the last two lectures we introduced the fundamental unit of quantum information - the qubit, and the postulates of quantum mechanics that govern how the state of a qubit can change. In this lecture, we will present the no-cloning theorem, a consequence of the postulates that says arbitrary quantum states cannot be copied. Then, we will show how entanglement can be used to share quantum information in spite of the no-cloning theorem's restriction. Lastly we will present BB84 a simple quantum cryptography protocol for key distribution.

2 No-cloning Theorem

The no-cloning theorem states that it is impossible to create a copy of an arbitrary quantum state. Consider a quantum computer with two registers: the *data register* which is in state $|\psi\rangle$, and the *target register* which is in a particular state $|t\rangle$. Then, the no-cloning theorem is equivalent to saying that for every state $|\psi\rangle$, there is no unitary quantum circuit U that can transform the state to

$$|\psi\rangle \otimes |t\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \,. \tag{2.1}$$

Okay, so we can't copy arbitrary states with a quantum computer, but since we know that we can copy classical data, there must be some sort of restriction on the quantum states that we can copy. Let's assume there is a unitary U that is described by equation 2.1. Then for two quantum states $|\psi\rangle$ and $|\phi\rangle$, we have

$$U(|\psi\rangle \otimes |t\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{2.2}$$
$$U(|\phi\rangle \otimes |t\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{2.3}$$

Now let's take the inner product of equations 2.2 and 2.3:

$$(\langle\psi| \otimes \langle t|)U^\dagger U(|\phi\rangle \otimes |t\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) \tag{2.4}$$
$$(\langle\psi| \otimes \langle t|)(|\phi\rangle \otimes |t\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) \tag{2.5}$$
$$\langle\psi|\phi\rangle \langle t|t\rangle = \langle\psi|\phi\rangle \langle\psi|\phi\rangle \tag{2.6}$$
$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \tag{2.7}$$

So, the only solutions for this are $\langle\psi|\phi\rangle = 0, 1$. This tells us that we can build a circuit that can clone orthogonal states only. An example of this is the CNOT gate:

$$\text{CNOT}(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \tag{2.8}$$
$$\text{CNOT}(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle \tag{2.9}$$

Now let's try copying an arbitrary state with the CNOT gate.

$$\text{CNOT}(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle = \alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |1\rangle) \tag{2.10}$$

You can see that this isn't a copy of the state we wished to copy, the statevector of two copies of that state is the following.

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha^2(|0\rangle \otimes |0\rangle) + \alpha\beta(|0\rangle \otimes |1\rangle) + \alpha\beta(|1\rangle \otimes |0\rangle) + \beta^2(|1\rangle \otimes |1\rangle) \tag{2.11}$$

Note how an arbitrary state doesn't get copied by the CNOT, only the $|0\rangle$ and $|1\rangle$ states.

3 Quantum Teleportation

Because of the no-cloning theorem, it's impossible to send a copy of a quantum state to someone else. We can however, send the state of our quantum system to someone else with the help of quantum entanglement.

Suppose Alice and Bob share an entangled pair of qubits in the state

$$|\Psi\rangle_{AB} = \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}} \tag{3.1}$$

The subscript A denotes that it is Alice's qubit, and B denotes Bob's qubit. Suppose Alice has another qubit (labelled with subscript C) in the state

$$|\psi\rangle_C = \alpha |0\rangle_C + \beta |1\rangle_C \tag{3.2}$$

The following quantum circuit moves the state $|\psi\rangle$ to Bob's qubit:

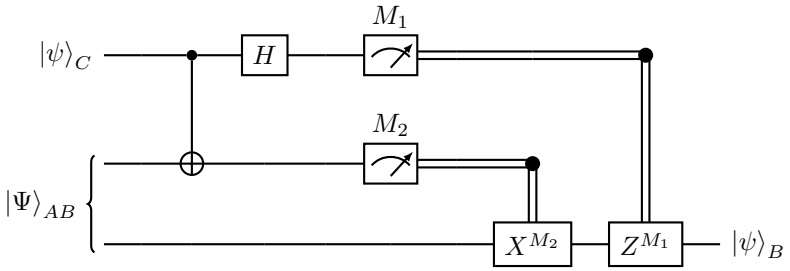

Figure 3.1: The qubit teleportation circuit. From top to bottom, the qubits are C, A, B. You can find the Qiskit implementation of this circuit in the appendix.

Initially the whole system is in the state

$$\begin{aligned} |\psi\rangle_C |\Psi\rangle_{AB} &= (\alpha |0\rangle_C + \beta |1\rangle_C) \otimes \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B) \\ &= \frac{1}{\sqrt{2}} (\alpha |0\rangle_C |0\rangle_A |0\rangle_B + \beta |1\rangle_C |0\rangle_A |0\rangle_B + \alpha |0\rangle_C |1\rangle_A |1\rangle_B + \beta |1\rangle_C |1\rangle_A |1\rangle_B) \end{aligned}$$

After Alice applies the CNOT and Hadamard gates, the system evolves as such:

$$\begin{aligned} |\psi\rangle_C |\Psi\rangle_{AB} &\xrightarrow{\text{CNOT}_{C,A}} \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha |0\rangle_C |0\rangle_A |0\rangle_B \\ +\beta |1\rangle_C |1\rangle_A |0\rangle_B \\ +\alpha |0\rangle_C |1\rangle_A |1\rangle_B \\ +\beta |1\rangle_C |0\rangle_A |1\rangle_B \end{pmatrix} \\ &\xrightarrow{H_C} \frac{1}{2} \begin{pmatrix} \alpha(|0\rangle_C + |1\rangle_C) |0\rangle_A |0\rangle_B \\ +\beta(|0\rangle_C - |1\rangle_C) |1\rangle_A |0\rangle_B \\ +\alpha(|0\rangle_C + |1\rangle_C) |1\rangle_A |1\rangle_B \\ +\beta(|0\rangle_C - |1\rangle_C) |0\rangle_A |1\rangle_B \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} |0\rangle_C |0\rangle_A (\alpha |0\rangle_B + \beta |1\rangle_B) \\ + |0\rangle_C |1\rangle_A (\beta |0\rangle_B + \alpha |1\rangle_B) \\ + |1\rangle_C |0\rangle_A (\alpha |0\rangle_B - \beta |1\rangle_B) \\ + |1\rangle_C |1\rangle_A (-\beta |0\rangle_B + \alpha |1\rangle_B) \end{pmatrix} \end{aligned}$$

Now Alice takes a measurement on qubits C and A and records the measurements as M_1 and M_2 respectively. She sends Bob these measurements via a classical communication channel. The table below shows how Bob corrects his qubit's state to be $|\psi\rangle$ after he receives the measurements from Alice.

M_1	M_2	State of Qubit B	Corrective Gate
0	0	$\|\psi\rangle$	I
0	1	$X\|\psi\rangle$	X
1	0	$Z\|\psi\rangle$	Z
1	1	$XZ\|\psi\rangle$	ZX

Note that this process does not violate the no-cloning theorem. The state of Alice's qubit C collapsed due to the measurement. Because Alice does not need to use any quantum communication channel to transfer the state information from qubit C to qubit B, we say that the state of qubit C *teleports* to Bob's qubit B. So, we call this process *quantum teleportation*.

4 Superdense Coding

When two or more qubits are in an entangled state, measuring or applying a gate to of one of the qubits will affect the state of the entire system of qubits even if the qubits are not physically near each other. We can make use of this fact to seemingly encode two bits of information via a single qubit, part of an entangled pair, this is called *superdense coding*.

Alice and Bob each have one qubit each from an entangled pair in the state

$$\frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}}. \tag{4.1}$$

Table 4.1 shows the encoding scheme for bit-strings to operators and what state the entangled pair will be in after the gate is applied to Alice's qubit.

Bit String	Gate	Final State
00	I	$(\|0\rangle_A \|0\rangle_B + \|1\rangle_A \|1\rangle_B)/\sqrt{2}$
01	Z	$(\|0\rangle_A \|0\rangle_B - \|1\rangle_A \|1\rangle_B)/\sqrt{2}$
10	X	$(\|1\rangle_A \|0\rangle_B + \|0\rangle_A \|1\rangle_B)/\sqrt{2}$
11	ZX	$(-\|1\rangle_A \|0\rangle_B + \|0\rangle_A \|1\rangle_B)/\sqrt{2}$

Table 4.1: Superdense coding bit-encoding scheme.

The final states are called Bell states and together form the *Bell basis*. Alice applies the gate corresponding to the two bits she wants to send Bob, and then sends her qubit of the entangled pair to Bob via a quantum channel. Since the Bell basis is orthogonal, Bob can take a measurement in the Bell basis and learn which bit string Alice meant to send him by referring to the same table.

Note that Alice is NOT encoding two bits of information into a single qubit. A single qubit can only be measured to give a single bit of information. Instead, Alice is encoding two bits of information into a system of two spatially separated qubits – the entangled pair. Because their qubits are entangled, Alice is able to change the state of the whole system by applying gates to only her own qubit.

5 Quantum Key Distribution (BB84)

In this section, we will look at a practical application for quantum communication – *quantum key distribution*. If you use any messaging app with end-to-end encryption, in order to protect the messages you're sending to your friend from prying eyes, the app generates an *encryption key* using which the messages are encrypted and decrypted. This encryption key must be shared by both you and your friend, the procedure by which the messaging app's backend gives both parties the encryption key is called *key distribution*. In classical key distribution, whoever generates the key must find a way to send it to the other party. But, how are we to trust that nobody else was able to intercept the distribution learn the key? The security of your messages depends on the security of your key distribution, and classically, there is no way to guarantee the security of the key distribution. With access to a quantum communication channel,

The BB84 Protocol

Defining the key

Let's say Alice and Bob want to generate an encryption key and they have access to a quantum communication channel. To make things simple, let's say that the key is just a string of 5 bits that both Alice and Bob can agree upon. In practice though, actual encryption keys will be much longer than 5 bits and will have certain constraints, the procedure we will describe below can be extended to generate those keys too.

Initialize Qubits

Alice has 5 qubits that she will send to Bob. She can initialize each of her qubits in one of 4 states: $|0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$. $R = \{r_0 = |0\rangle, r_1 = |1\rangle\}$ form the *rectangular basis*, and $D = \{d_0 = |+\rangle, d_1 = |-\rangle\}$ form the *diagonal basis*. For each qubit, Alice will randomly choose a basis R or D and also randomly choose a bit 0 or 1. She will prepare each qubit corresponding to the basis and bit and make note of this information before sending the qubits to Bob via a quantum channel (assume that the channel is ideal, i.e. it does not change the state of the qubits going through it).

Make Measurements

For each qubit Bob receives, he randomly chooses a basis R or D and measures the qubit in the corresponding basis. Bob makes note of the basis and the measured bit. A D-basis measurement of $|+\rangle$ is noted as 0 and $|-\rangle$ is noted as 1.

Generate Key

Alice sends Bob the list of bases she initialized each qubit in, and Bob sends Alice the list of bases he measured each qubit in via a classical channel and use this information to generate the bits of their key.

- If Bob measured in the same basis than what Alice initialized a qubit in, he will have measured the same bit that Alice initialized. So, they each record their bit as part of the encryption key.
- If Bob measured in a different basis than what Alice initialized a qubit in, Bob's measurement will randomly be 0 or 1 with equal probability. They ignore their bit in this case.

Alice and Bob will repeat these steps until they have enough bits to form the key.

An example of one round of this protocol is shown in Table 5.1.

With a classical channel, an eavesdropper Eve can copy the bits going to Bob without Bob finding out, the no-cloning theorem prevents her from doing the same in a quantum channel. Moreover, to learn any information about a qubit she has intercepted, Eve must make a measurement, which will alter the state of the qubit before Bob receives it. If Eve does make a measurement, then Bob's bits will not perfectly match Alice's bits and so they will each have different keys. Since Alice and Bob will be using their respective keys to do further communication, they will easily notice if their keys don't match, and they can find a new channel to generate a new key.

Alice			Bob			Accept Bit?
Qubit State	Basis Choice	Bit	Basis Choice	Measured State	Bit	
$\|0\rangle$	R	0	R	$\|0\rangle$	0	✔
$\|1\rangle$	R	1	D	$\|+\rangle$	0	✘
$\|+\rangle$	D	0	R	$\|1\rangle$	1	✘
$\|-\rangle$	D	1	D	$\|-\rangle$	1	✔
$\|+\rangle$	D	0	D	$\|+\rangle$	0	✔

Table 5.1: An example round of the BB84 protocol. At the end of this round both Alice and Bob agree that their key begins with "010".