Lecture 3

Sharing Quantum States

Swagat Kumar and Emilio Peláez

The Eigensolvers Quantum School

TABLE OF CONTENTS

No-Cloning Theorem

It is **impossible** to create a copy of an arbitrary quantum state. In other words, there is no unitary circuit U such that

$$|\psi\rangle \otimes |t\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \,, \tag{1}$$

for any state $|t\rangle$.

But we know we **can** copy classical information. You can easily make two copies of an arbitrary string in a classical computer. You can even see this in the circuit model with the FANOUT gate.

No-Cloning Theorem

Let's assume a unitary like that in Eq. (1) is possible. Thus, for two states we have

$$U(|\psi\rangle \otimes |t\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{2}$$
$$U(|\phi\rangle \otimes |t\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{3}$$

Taking the inner product of these we get

$$(\langle\psi| \otimes \langle t|)U^\dagger U(|\phi\rangle \otimes |t\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) \tag{4}$$
$$(\langle\psi| \otimes \langle t|)(|\phi\rangle \otimes |t\rangle) = (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) \tag{5}$$
$$\langle\psi|\phi\rangle \langle t|t\rangle = \langle\psi|\phi\rangle \langle\psi|\phi\rangle \tag{6}$$
$$\langle\psi|\phi\rangle = (\langle\psi|\phi\rangle)^2 \tag{7}$$

What values satisfy this?

No-Cloning Theorem

The only solutions are $\langle\psi|\phi\rangle = 0, 1$. Therefore, there exists some type of U: it can only clone **orthogonal states**.

Take for example the CNOT gate.

$$\text{CNOT}(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle \tag{8}$$
$$\text{CNOT}(|1\rangle \otimes |0\rangle) = |1\rangle \otimes |1\rangle \tag{9}$$

But if we try with an arbitrary state, it is **not** cloned.

$$\text{CNOT}((\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle) = \alpha(|0\rangle \otimes |0\rangle) + \beta(|1\rangle \otimes |1\rangle) \tag{10}$$

No-Cloning Theorem

Questions?

Quantum Teleportation

We cannot send a copy of our state, but we can send our state itself by exploiting quantum entanglement.

Suppose Alice wants to send her quantum state, which we call $|\psi\rangle_C$ to Bob.

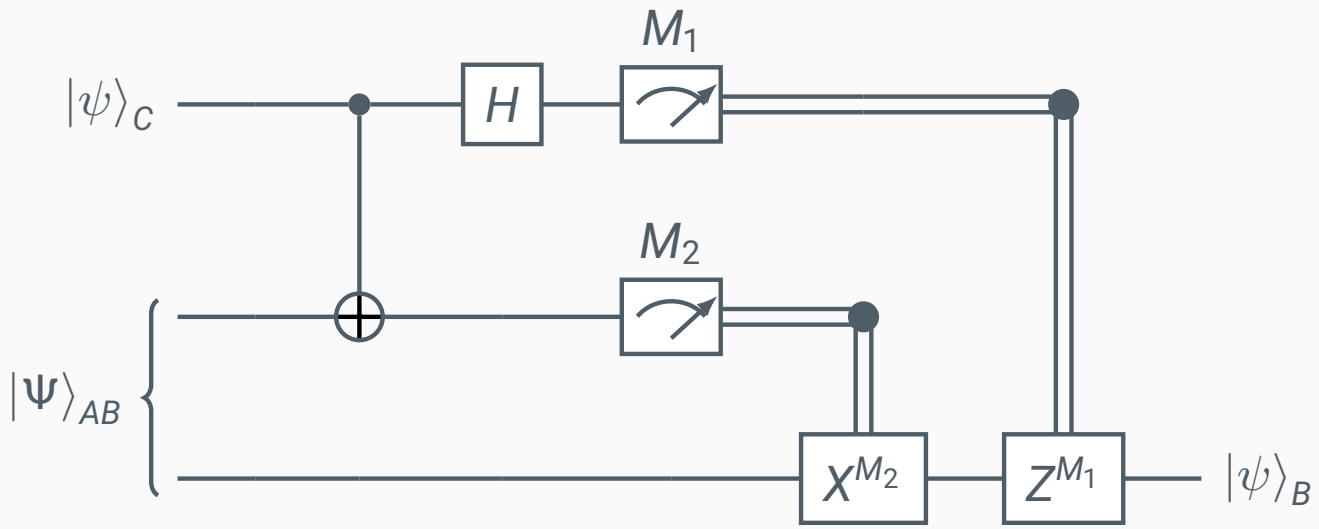
$$|\psi\rangle_C = \alpha\,|0\rangle_C + \beta\,|1\rangle_C \tag{11}$$

Additionally, each of them has a qubit of the following entangled state they shared beforehand.

$$|\Psi\rangle_{AB} = \frac{|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B}{\sqrt{2}} \tag{12}$$

Quantum Teleportation

The circuit to send state $|\psi\rangle_C$ from Alice to Bob is the following.



Quantum Teleportation

The initial state is

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

After the CNOT gate, we get

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

Quantum Teleportation

And after the *H* gate on $|\psi\rangle_C$ we get

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

Which we can simplify to

$$
\begin{aligned}
\frac{1}{2}(&|0\rangle_C |0\rangle_A (\alpha|0\rangle_B + \beta|1\rangle_B) \\
&+ |0\rangle_C |1\rangle_A (\beta|0\rangle_B + \alpha|1\rangle_B) \\
&+ |1\rangle_C |0\rangle_A (\alpha|0\rangle_B - \beta|1\rangle_B) \\
&+ |1\rangle_C |1\rangle_A (-\beta|0\rangle_B + \alpha|1\rangle_B))
\end{aligned}
$$

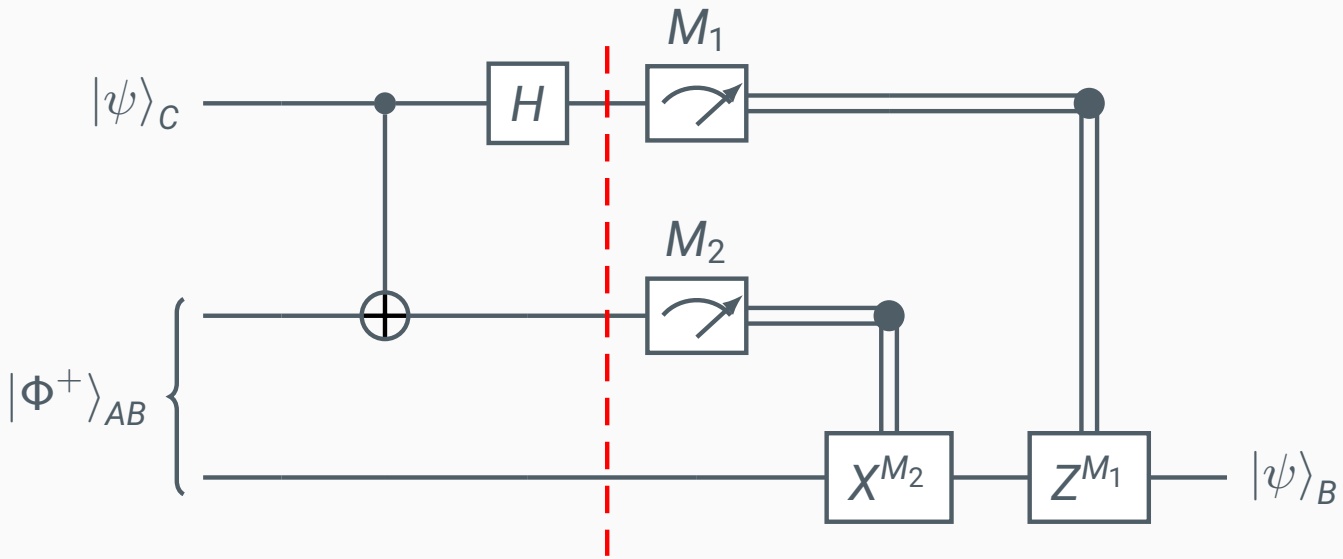
Quantum Teleportation

This simplification may not seem evident at first sight, so let's do it step by step.

$$\frac{1}{2}(\alpha(|0\rangle_C + |1\rangle_C)\,|0\rangle_A\,|0\rangle_B + \beta(|0\rangle_C - |1\rangle_C)\,|1\rangle_A\,|0\rangle_B \\ + \alpha(|0\rangle_C + |1\rangle_C)\,|1\rangle_A\,|1\rangle_B + \beta(|0\rangle_C - |1\rangle_C)\,|0\rangle_A\,|1\rangle_B)$$

Quantum Teleportation

We are up to here in the teleportation circuit



Quantum Teleportation

The possible measurements are summarized in the following table.

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

The corrective gates are applied to qubit B after measuring qubits A and C.

Quantum Teleportation

1. $M_1 = 0$ and $M_2 = 0$. $|C\rangle = \alpha |0\rangle_C + \beta |1\rangle_C$. Corrective gate: I.

2. $M_1 = 0$ and $M_2 = 1$. $|C\rangle = \alpha |1\rangle_C + \beta |0\rangle_C$. Corrective gate: X.

3. $M_1 = 1$ and $M_2 = 0$. $|C\rangle = \alpha |0\rangle_C - \beta |1\rangle_C$. Corrective gate: Z.

4. $M_1 = 1$ and $M_2 = 1$. $|C\rangle = \alpha |1\rangle_C - \beta |0\rangle_C$. Corrective gate: ZX.

Quantum Teleportation

Although the state $\alpha|0\rangle + \beta|1\rangle$ was sent from qubit *C* to qubit *B*, we did not **violate** the no-cloning theorem.

The state on Alice's qubit *C* collapsed due to the measurement we performed. Therefore, two copies of the state don't exist at the same time anywhere in the protocol.

It is called teleportation since physical qubits were never exchanged between Alice and Bob (except for the entangled pair, but that can be done even before having $|\psi\rangle$). Only classical information was exchanged.

Questions?

Superdense Coding

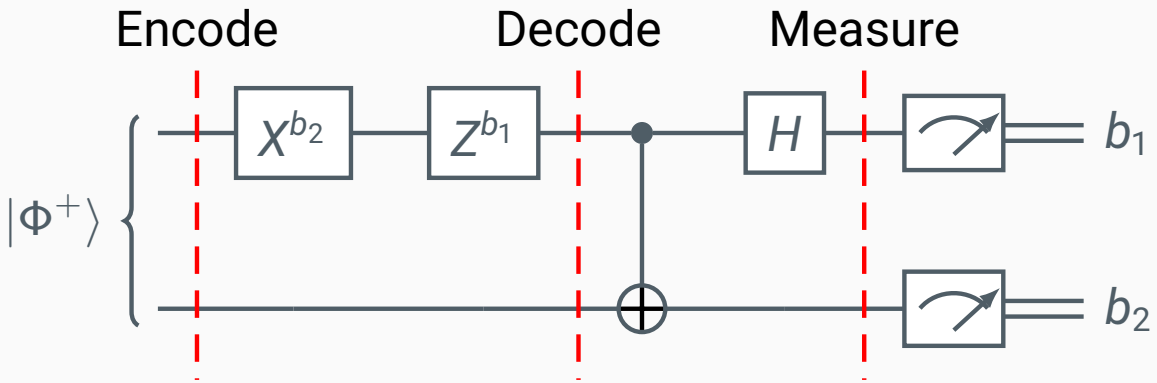
Superdense coding is a quantum communication protocol that allows us to send two bits of classical information by physically moving one qubit.

When you apply a gate to one qubit from an entangled pair, the other qubit will be affected no matter the physical distance between them. This protocol exploits that fact to encode classical information in a pair of entangled qubits.

Superdense coding applies gates to one qubit but is able to communicate two bits of information. However, Alice is **not** encoding two bits of information into a single qubit. She is just taking advantage of entanglement.

Superdense Coding

The complete circuit for superdense coding is the following. The initial state we send through the circuit is the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. And the classical bitstring we want to send $b = b_1 b_2$.



Although the wires here seem to be physically together all the time, they can be as far apart as you want during the encoding process. However, they need to be back together for the CNOT gate in the decoding process and the measurement.

Superdense Coding

1. $b = 00$. Encoding gate $= I$.

2. $b = 01$. Encoding gate $= X$.

3. $b = 10$. Encoding gate $= Z$.

4. $b = 11$. Encoding gate $= ZX$.

Superdense Coding

The two final steps, decoding and measurement, can be seen as one single step: measurement on the Bell basis. This can be thought of as the reverse of encoding the four Bell states. Encoding Bell states look as follows:

$$|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{13}$$

$$|01\rangle \rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{14}$$

$$|10\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{15}$$

$$|11\rangle \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{16}$$

To perform measurement on the Bell basis, just invert the direction of the arrows.

Superdense Coding

Questions?

Quantum Key Distribution

In most cryptographic models, an encryption key needs to be shared between two parties. A problem with this is that these parties need to make sure that no one intercepts it. If the key is intercepted, the security of the model and the information sent through it is compromised.

Quantum computers can help us develop a secure channel to share this key. BB84 is a quantum protocol that allows two users to share a key safely with each other.

Quantum Key Distribution

Alice starts off with 5 qubits that she can initialize one of these states:

$$|0\rangle,\ |1\rangle,\ |+\rangle,\ |-\rangle \tag{17}$$

The first two states form the **rectangular** (R) basis and the last two form the **diagonal** (D) basis. For each qubit, Alice chooses a basis and a bit 0 or 1.

$$R = \{0 = |0\rangle,\ 1 = |1\rangle\}$$
$$D = \{0 = |+\rangle,\ 1 = |-\rangle\}$$

After initializing her qubits, she sends them to Bob through an **ideal** quantum channel.

Quantum Key Distribution

Once Bob receives the qubit, he randomly chooses a basis (*R* or *D*) and measures it. After Bob finishes measuring, Alice and Bob share with each other the basis they chose. For each qubit there are two possibilities:

- Bob and Alice chose the same basis $\rightarrow$ they record the corresponding bit to their encryption key
- Bob and Alice chose different basis $\rightarrow$ they discard the corresponding bit

This process is repeated until enough bits are recorded for their key.

Quantum Key Distribution

The following table shows how a small example of this protocol would go.

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

Quantum Key Distribution

We know that someone looking into the quantum channel Alice and Bob use to send qubits can't copy their qubits because of the no-cloning theorem. But what if an eavesdropper, called Eve, measures the qubits and puts them back on the channel?

In this case, Alice and Bob have a way of noticing the presence of Eve. Since measurement collapses the quantum state, and Eve doesn't know what basis Alice used to encode, Eve only has 50% chance of choosing the right basis. But even if Eve chooses the wrong basis, at the end Bob will measure the intended state with 50% chance.

This may seem like a high probability that Eve is able to measure the qubits and go unnoticed. But the keys Alice and Bob will send are hundred of bits long. Sooner or later, Alice and Bob will notice Eve's presence with high probability.

Quantum Key Distribution

To notice Eve, Alice and Bob have to share some bits of their final key in addition to the bases they used.

After sharing their bases and discarding the bits in which they don't coincide, Alice and Bob randomly select some bits out of their resulting key and compare them. If Eve didn't interfere and therefore didn't mess up the states, then they should see their bits are the same. But if they see that their bits are not exactly the same, they will someone measured the qubits before Bob.

Quantum Key Distribution

Now, let's look at an example where Eve is able to intercept the qubits sent from Alice to Bob and go unnoticed.

Alice	Eve		Bob		
Qubit State	Basis	Measured	Basis	Measured	Bit
$\|0\rangle$	D	$\|-\rangle$	R	$\|0\rangle$	0
$\|1\rangle$	R	$\|1\rangle$	R	$\|1\rangle$	1
$\|+\rangle$	D	$\|+\rangle$	R	$\|1\rangle$	1
$\|-\rangle$	D	$\|-\rangle$	D	$\|-\rangle$	1
$\|+\rangle$	R	$\|0\rangle$	D	$\|+\rangle$	0

Quantum Key Distribution

In a more realistic situation, Eve would be noticed after a few bits.

Alice	Eve		Bob		
Qubit State	Basis	Measured	Basis	Measured	Bit
$\|0\rangle$	D	$\|-\rangle$	R	$\|0\rangle$	0
$\|1\rangle$	R	$\|1\rangle$	R	$\|1\rangle$	1
$\|+\rangle$	D	$\|+\rangle$	R	$\|1\rangle$	1
$\|-\rangle$	D	$\|-\rangle$	D	$\|-\rangle$	1
$\|+\rangle$	R	$\|0\rangle$	D	$\|-\rangle$	1

Questions?