Quantum Entanglement Presentation Notes

Francesco Stern

February 2024

1 Quantum Teleportation (Chapter 5.8)

An unknown Quantum State can be teleported from one location to another.
As much as it may sound like sci-fi, Yes, it is possible, in quantum mechanics, to teleport the state of one qubit to another one.

First, let's visualize this in circuit notation:

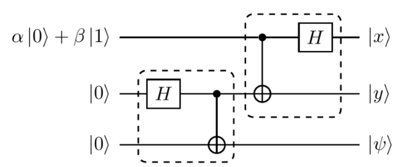

Figure 1: Quantum Teleportation circuit

Let's imagine two fellow PhD students, Alice and Bob, who are both running experiments on quantum states. Alice, who goes to Columbia, is in possession of 3 qubits, one of which is in a very precious quantum state, and the other two which are entangled.

Bob, who goes to Cornell, is coming to pick the first qubit up because he needs it for an experiment. He gets to Columbia, picks up the qubit, and leaves. Once he is back in his lab, he and Alice realize that she gave him not the qubit he wanted but one of the entangled ones.

Is there a way for Alice, through a classical broadcast, to rectify her monumental mistake? Yes!

Our first cubit we suppose to be in an arbitrary state $\alpha \mid 0\rangle + \beta \mid 1\rangle$ and, after entangling our two following cubits with the Hadamard and C-NOT gates, we will have them in a Bell State, say $\mid \Omega\rangle = \mid 00\rangle + \mid 11\rangle$.

Now, the state of the three-qubit system will then read

$$| \ 00\rangle + | \ 11\rangle \otimes \alpha \mid 0\rangle + \beta \mid 1\rangle \tag{1}$$

What Alice can do, given that the Bell States form an orthonormal basis of our four-dimensional Hilbert Space, is rewrite Formula (1) in Bell basis, and thus obtain this

$$
\begin{aligned}
&| \ 00\rangle + | \ 11\rangle \otimes \alpha \mid 0\rangle + \beta \mid 1\rangle \\
+ &| \ 01\rangle + | \ 10\rangle \otimes \alpha \mid 1\rangle + \beta \mid 0\rangle \\
+ &| \ 00\rangle - | \ 11\rangle \otimes \alpha \mid 0\rangle - \beta \mid 1\rangle \\
+ &| \ 01\rangle - | \ 10\rangle \otimes \alpha \mid 1\rangle - \beta \mid 0\rangle
\end{aligned}
$$

Once Alice has her system expressed in Bell basis, she can then perform our Bell Measurement, as illustrated graphically by the C-NOT + Hadamard Gates in Figure 1.
What the Bell Measurement allows Alice to do is to map the Bell States back to their counterparts in computational basis, and thus allows her to write the previous expression as

$$
\begin{aligned}
&| \ 00\rangle \otimes \alpha \mid 0\rangle + \beta \mid 1\rangle \\
+ &| \ 01\rangle \otimes \alpha \mid 1\rangle + \beta \mid 0\rangle \\
+ &| \ 10\rangle \otimes \alpha \mid 0\rangle - \beta \mid 1\rangle \\
+ &| \ 11\rangle \otimes \alpha \mid 1\rangle - \beta \mid 0\rangle
\end{aligned}
$$

Then, once she performs the standard measurement and obtains x and y, she communicates them to Bob, who associates them to one of the following transformations:

$$
\begin{aligned}
&| \ 00\rangle \mapsto Id \\
&| \ 01\rangle \mapsto X \\
&| \ 10\rangle \mapsto Z \\
&| \ 11\rangle \mapsto ZX
\end{aligned}
$$

.

At this point, Bob only needs to apply whatever transformation he obtains to the qubit in his possession and he will restore it to the state of the first qubit.

Is this only theoretical? No! In fact, the first successful experiment involving Quantum Teleportation was done in 1997. The world record in terms of distance, however, was achieved in 2017, when Quantum Teleportation was performed between Earth and a satellite 1400km in orbit.

Now, it is important to note that, in performing our Bell Measurement, the state of our first qubit, the one in Alice's possession, is destroyed, which leads us into the topic of quantum cloning, the no-cloning theorem, and other no-go theorems.

2 No-Cloning and other No-Go Theorems (Chapter 5.9)

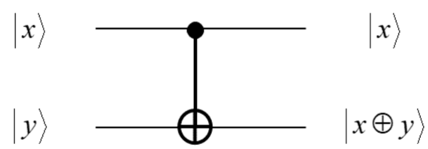

Figure 2: c-NOT gate

As Naomi has shown earlier, the c-NOT gate acts on two qubits in a basis state in a way that makes it seem like the target qubit "learns" about the state of the control qubit, giving us this mapping:

$$|\ x\rangle\ |\ 0\rangle \mapsto |\ x\rangle\ |\ x\rangle \tag{2}$$

What this kind of looks like then is that the first qubit is being "cloned". Let's see if this statement holds.
Let's take a qubit in an arbitrary quantum state $|\ \psi\rangle = \alpha\ |\ 0\rangle\ + \beta\ |\ 1\rangle$.
Now, let's assume that there exists a Unitary Quantum operator such that $|\ \psi\rangle\ |\ 0\rangle \mapsto |\ \psi\rangle\ |\ \psi\rangle$.
If we compute the right part we get
$|\ \psi\rangle\ |\ \psi\rangle = (\alpha\ |\ 0\rangle\ + \beta\ |\ 1\rangle)(\alpha\ |\ 0\rangle\ + \beta\ |\ 1\rangle) = \alpha^2\ |\ 00\rangle\ + \alpha\beta\ |\ 01\rangle +$
$+\ \beta\alpha\ |\ 10\rangle + \beta^2\ |\ 11\rangle$.
Instead, if we compute the left part, we get
$|\ \psi\rangle\ |\ 0\rangle = (\alpha\ |\ 0\rangle\ + \beta\ |\ 1\rangle)\ |\ 0\rangle = \alpha\ |\ 00\rangle + \beta\ |\ 11\rangle$.

Since there are no cross terms in our second equation, we have a contradiction against the linearity condition of quantum mechanics, and there thus cannot exist such a Unitary Quantum Operator.

The "No-Cloning Theorem" thus states:
There is no Unitary operator U on $H \otimes H$ such that, for all normalized states $|\ \psi\rangle_A$ and $|\ e\rangle_B$ in H, $U(|\ \psi\rangle_A\ |\ e\rangle_B) = e^{i\alpha(\psi,e)}\ |\ \psi\rangle_A\ |\ \psi\rangle_B$.

The "No-Cloning Theorem is one of a number of other "No-Go Theorems" in Quantum Computing, which we will now mention:

- **No-Teleportation Theorem** An arbitrary quantum state cannot be entirely expressed with classical information, i.e. the process of converting quantum information into classical cannot be reversed.

  This can be seen as a consequence of no-cloning: if we were able to turn a quantum state into classical information and then back again, we could simply clone the classical information and then get a cloned copy of our quantum state.

Note that this theorem refers to the idea of *Classical* teleportation, whereas the Teleportation that we have seen earlier, which we achieve by entanglement, is *quantum* teleportation

- **No-Broadcasting** Given a single copy of a quantum state, it cannot be shared with two or more parties.

  Note that, if we are given more than one copy of a single quantum state to begin with, then this does not hold.
  In fact, it has been proven that if we are given four or more copies of a quantum state, one can purify the state while broadcasting, giving birth to a phenomenon that is called *Superbroadcasting*

- **No-Deleting Theorem** Given two copies of an arbitrary quantum state, it is impossible to delete one.

The theorem holds for quantum states in a Hilbert space of any dimension. For simplicity, consider the deleting transformation for two identical qubits. If two qubits are in orthogonal states, then deletion requires that

$$|0\rangle_A|0\rangle_B|A\rangle_C \to |0\rangle_A|0\rangle_B|A_0\rangle_C,$$
$$|1\rangle_A|1\rangle_B|A\rangle_C \to |1\rangle_A|0\rangle_B|A_1\rangle_C.$$

Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ be the state of an unknown qubit. If we have two copies of an unknown qubit, then by linearity of the deleting transformation we have

$$|\psi\rangle_A|\psi\rangle_B|A\rangle_C = [\alpha^2|0\rangle_A|0\rangle_B + \beta^2|1\rangle_A|1\rangle_B + \alpha\beta(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)]|A\rangle_C$$
$$\to \alpha^2|0\rangle_A|0\rangle_B|A_0\rangle_C + \beta^2|1\rangle_A|0\rangle_B|A_1\rangle_C + \sqrt{2}\alpha\beta|\Phi\rangle_{ABC}.$$

In the above expression, the following transformation has been used:

$$1/\sqrt{2}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)|A\rangle_C \to |\Phi\rangle_{ABC}.$$

However, if we are able to delete a copy, then, at the output port of the deleting machine, the combined state should be

$$|\psi\rangle_A|0\rangle_B|A'\rangle_C = (\alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|0\rangle_B)|A'\rangle_C.$$

In general, these states are not identical and hence we can say that the machine fails to delete a copy. If we require that the final output states are same, then we will see that there is only one option:

$$|\Phi\rangle = 1/\sqrt{2}(|0\rangle_A|0\rangle_B|A_1\rangle_C + |1\rangle_A|0\rangle_B|A_0\rangle_C),$$

and

$$|A'\rangle_C = \alpha|A_0\rangle_C + \beta|A_1\rangle_C.$$

Figure 3:

  Thus, because the final state of the ancilla is normalized for all α, β, the two initial states must be orthogonal, which means that we are not actually "deleting" any quantum information, but merely swapping it onto a two-dimensional subspace of the ancilla.

- **No-Communication Theorem** An entangled state cannot be used to transmit information by measurement of a subsystem.

- **No-Hiding Theorem** Quantum Information cannot be lost, even through decoherence.

3 Controlled-phase and Controlled-U (Chapter 5.10

We have seen the c-NOT gate, but that is not the only two-qubit gate. In this chapter, we will explore two other two-qubit gates, the Controlled-phase and Controlled-U gate.

We begin with the Controlled-phase gate c-P_φ, which we represent in Matrix notation as:

Controlled-phase	$\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{array}\right]$

Figure 4: Enter Caption

and in circuit notation as:

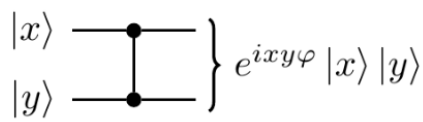

Figure 5: controlled-phase gate, $x, y \in \{0, 1\}$

To see the entangling power of this gate, let us look at the following circuit:

Now, in this circuit, what the Hadamard gates do is they prepare an equally weighted superposition of the states from our computational basis $\{|\,00\rangle + |\,01\rangle + |\,10\rangle + |\,11\rangle\}$, which we write $\frac{1}{2}(|\,00\rangle + |\,01\rangle + |\,10\rangle + |\,11\rangle)$

.

Taking the phase $\varphi = \pi$, what we obtain is a gate that we call the controlled-Z operator (in reference to the Z bit-flip operation), which acts on our superposition by flipping the sign on our last term, giving $\frac{1}{2}(|\,00\rangle + |\,01\rangle + |\,10\rangle - |\,11\rangle)$

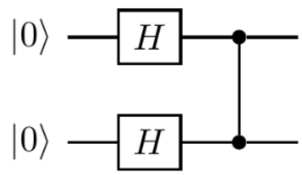

Figure 6: Enter Caption

As it turns out, both the c-NOT and the c-P_φ gates are specific forms of the more general construction of the controlled-U gate (where U is an arbitrary single-qubit unitary transformation), written in matrix form as follows:

Controlled-U $\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{U}} \\ 0 & 0 & & \end{array}\right]$

Figure 7: Enter Caption

and in circuit form:

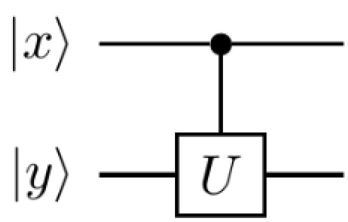

Figure 8: controlled-U gate, $x, y \in \{0, 1\}$

4 Universality, revisited (5.11)

Now that we have introduced phase gates, the Hadamard gates and c-NOT, we can introduce the concept of a Universal set of gates.
A Universal Set of Gates is a set composed by gates that can be used to approximate to any degree of accuracy any unitary operation on a quantum Computer. One example of such set, which we will see again in the future, is the set formed

by the Hadamard, c-NOT and T ($P_{\frac{\pi}{4}}$).

5 Phase kick-back (Chapter 5.12)

This section is going to come in handy later, when we introduce Quantum Algorithms, because we will see that this is the way that they create phase shifts.

We start with the following circuit:

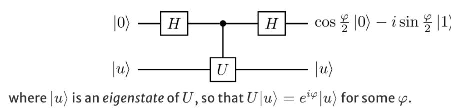

Figure 9: Controlled-U Interference

This circuit may seems familiar as it effectively is the same as our interference circuit (Hadamard - Phase Shift - Hadamard), the only change being that instead of the explicit phase shift we have a Controlled-U Gate.
Before diving into the computational aspect of the circuit, note that the second qubit is in a state $\mid u\rangle$, required to be an eigenstate of U.

First we have the Hadamard Gate:

$\mid 0\rangle \mid u\rangle \mapsto (\mid 0\rangle + \mid 1\rangle) \mid u\rangle = \mid 0\rangle \mid u\rangle + \mid 1\rangle \mid u\rangle.$
Then proceed with the Controlled-U Gate:

$$\mid 0\rangle \mid u\rangle + \mid 1\rangle \mid u\rangle \mapsto \mid 0\rangle \mid u\rangle + \mid 1\rangle U \mid u\rangle = \mid 0\rangle \mid u\rangle + e^{i\varphi} \mid 1\rangle \mid u\rangle =$$

$$= (\mid 0\rangle + e^{i\varphi} \mid 1\rangle) \mid u\rangle$$

and, lastly, with the second Hadamard Gate:

$$(\mid 0\rangle + e^{i\varphi} \mid 1\rangle) \mid u\rangle \mapsto (\cos(\tfrac{\varphi}{2}) \mid 0\rangle - i \sin(\tfrac{\varphi}{2}) \mid 1\rangle) \mid u\rangle$$

Key takeaways form this interaction:

- The second qubit $\mid u\rangle$ does not get entangled with the first one
- $\mid u\rangle$ does, however, induce a phase shift on the first qubit

Now we dive into a little preview of things to come:

$$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & X \end{bmatrix} = \begin{array}{l} \quad |00\rangle\langle 00| \otimes \mathbf{1} \\ + |01\rangle\langle 01| \otimes \mathbf{1} \\ + |10\rangle\langle 10| \otimes \mathbf{1} \\ + |11\rangle\langle 11| \otimes X. \end{array}$$

Figure 10: x-controlled U-operation

Here we have the First Register being of size 2x2 (Identity Matrix top-left), and the second register being size 1 (the Identity and X).

Now, if the First Register is prepared in state $| 11\rangle$, then X will perform a bit-flip on the qubit in the second register; otherwise, nothing will happen.

If we prepare the qubit in the second register in a state $| 0\rangle - | 1\rangle$ (eigenstate of X), whenever X is applied to the second register, the phase factor -1 will appear in front of the corresponding term in the first register.

If we then prepare the first register in superposition $| 00\rangle + | 01\rangle + | 10\rangle + | 11\rangle$, then the result of applying the x-controlled-U operation will be the entangled state $| 00\rangle + | 01\rangle + | 10\rangle - | 11\rangle$.

What the Phase kick-back mechanism does then is it introduces a relative phase in the equally-weighted superposition of all binary strings of length two.

We will get back to this because phase kick-back is the way through which we can control quantum interference in quantum computing.