QuIC Seminar 2

The Quantum Teleportation Algorithm

Contents

2.1 Problem Setup

The problem that *quantum teleportation* looks to solve is as follows: Alice has an unknown qubit $|\psi\rangle$ that she wants to send to Bob. How can she do this?

It's interesting to note that this is non-trivial in quantum information science, whereas in classical information theory the problem is no problem at all. How can we do this classically (i.e., send an unknown classical bit)? We would simply "look at" the information (i.e., read it by some means) and then send a message to Bob containing that information.

Why can't we do this with a qubit? It's because when we make a measurement, we disturb the state of the system according to the following measurement postulate of quantum mechanics. We saw a special case of this in the previous lecture when we measured a qubit in the computational basis. Here, our measurement operators were $M_0 := |0\rangle\langle 0|$ and $M_1 := |1\rangle\langle 1|$, which we "sandwiched" between our qubit to get the probability of obtaining either the zero state ($\langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle$) or the probability of obtaining the one state ($\langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|1\rangle\langle 1|\psi\rangle$). These measurement operators are Hermitian and satisfy the *completeness relation* $M_0^\dagger M_0 + M_1^\dagger M_1 = I$.

Exercise 11: Verify that the operators $M_0 := |0\rangle\langle 0|$ and $M_1 := |1\rangle\langle 1|$ satisfy the completeness relation $M_0^\dagger M_0 + M_1^\dagger M_1 = I$.

Solution 4: Follows by direct computation.

General measurements in quantum mechanics are described by the following, which also provides a rule for the state of a quantum system after a measurement is made.

Definition 2.1 (Measurement Postulate of Quantum Mechanics). **Quantum measurements** are described by a collection $\{M_m\}$ of *measurement operators* that act on the space of the quantum system being measured (e.g., $\mathbb{C}^2$ for qubits) and satisfy the *completeness equation*

$$\sum_m M_m^\dagger M_m = I. \tag{2.1}$$

The index m refers to all measurement outcomes that may occur. If the state of the system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is given by

$$p(m) := \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{2.2}$$

The state of the system immediately after the measurement is given by

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{2.3}$$

This postulate tells us how general measurements occur in quantum computing, a special case of which we saw when measuring qubits in the computational basis in Definition 1.10.

For our particular example of quantum teleportation, (2.3) is the most relevant. This feature says that the state of Alice's qubit would change if she measured it. Thus, in the quantum case, she cannot simply read the information in the qubit and send that to Bob.

Example 1: Completeness Equation is about Preserving Probability.

Why do we require that measurement operators $\{M_m\}$ satisfy the completeness equation (2.1)? What does this mean? It really expresses the fact that the sum of measurement probabilities must be equal to one, i.e. $\sum_m p(m) = 1$.

To see this, we can write

$$\begin{aligned}\sum_m p(m) &= \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle \\ &= \langle\psi|\left(\sum_m M_m^\dagger M_m\right)|\psi\rangle.\end{aligned}$$

Thus if (2.1) holds, we have $\sum_m p(m) = \langle\psi|\psi\rangle = 1$, as desired.

Exercise 12: Suppose we measure the qubit $|+\rangle = H|0\rangle$ in the computational basis and obtain the zero outcome. What is the state immediately after this measurement? Using the irrelevance of global phase (Theorem 1.3), argue that the qubit is in the $|0\rangle$ state immediately after measurement.

So Alice cannot measure her qubit and send that information to Bob without disturbing the state. Perhaps she can simply copy the state $|\psi\rangle$ onto another qubit she has, say $|\phi\rangle$, and send this qubit to Bob? It turns out that in general this is not possible in quantum mechanics, as described by the *no-cloning theorem.* To understand this theorem (which deals with multiple qubits), we first need to understand quantum systems consisting of more than one qubit.

2.2 Multi-Qubit States

A quantum computer with just one qubit wouldn't be very powerful, even with superposition. Suppose we have two qubits in our quantum computer, denoted $|\psi\rangle$ and $|\phi\rangle$. The total state of the whole computer, $|\Psi\rangle$, is given as the *tensor product* of its qubits, $|\Psi\rangle = |\psi\rangle \otimes |\psi\rangle$. Since each qubit on our two-qubit computer can be in one of two states ($|0\rangle$ or $|1\rangle$), the possibilities for the state of the whole computer are

$$|\Psi\rangle = \begin{cases} |0\rangle \otimes |0\rangle \\ |0\rangle \otimes |1\rangle \\ |1\rangle \otimes |0\rangle \\ |1\rangle \otimes |1\rangle \end{cases} . \tag{2.4}$$

But because of superposition, any linear combination of these states is also a valid state on our two qubit quantum computer. That is to say—the states in (2.4) form a basis for all possible states on a two-qubit quantum computer:

$$|\Psi\rangle = a|0\rangle \otimes |0\rangle + b|0\rangle \otimes |1\rangle + c|1\rangle \otimes |0\rangle + d|1\rangle \otimes |1\rangle \tag{2.5}$$

such that the complex amplitudes satisfy $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

This example illustrates the following:

Theorem 2.1 (Bases for Tensor Product Spaces.). Let $|i\rangle_A$, $i = 0, 1, ..., M-1$ be a basis for the Hilbert space H_A and $|j\rangle_B$, $j = 0, 1, ..., N-1$ be a basis for the Hilbert space H_B. Then, the MN states $|i\rangle_A \otimes |j\rangle_B$ form a basis for the composite space $H_{AB} = H_A \otimes H_B$. That is, any state $|\psi\rangle_{AB} \in H_{AB}$ can be written

$$|\psi\rangle_{AB} = \sum_{i,j} \alpha_{i,j} |i\rangle_A \otimes |j\rangle_B \tag{2.6}$$

such that $\sum_{i,j} |\alpha_{i,j}|^2 = 1$. The size of the composite space H_{AB} is thus $|H_{AB}| = MN$.

This theorem generalizes our previous example of two qubits to arbitrary Hilbert spaces. (In our two qubit example, $H_A = H_B = \mathbb{C}^2$ and $|i\rangle_A = |j\rangle_B = \{|0\rangle, |1\rangle\}$.) A particular note is that the size of the composite space H_{AB} is the *product* of the sizes of H_A and H_B. This leads to *exponentially* large Hilbert spaces and the common saying: "Hilbert space is a big place."

Example 2: The size of a Hilbert Space of n Qubits.

How many basis states are there for the composite Hilbert space consisting of n qubits? Each qubit has a basis of size two, hence the composite space has 2^n basis states.

We can enumerate the basis states of n qubits with bit strings of length n:

$$|z_1\rangle \otimes |z_2\rangle \otimes \cdots \otimes |z_n\rangle \tag{2.7}$$

where each $z_i \in \{0, 1\}$. Because it's a bit tedious to write out all of the tensor products, shorthand notation is often used, listed below. First, we can just omit the tensor product symbols to write

$$|z_1\rangle|z_2\rangle \cdots |z_n\rangle := |z_1\rangle \otimes |z_2\rangle \otimes \cdots \otimes |z_n\rangle. \tag{2.8}$$

This is shorter, but not as short as it can be: often, we will only write one ket for such a state and separate the bits z_i with commas,

$$|z_1, z_2, ..., z_n\rangle := |z_1\rangle \otimes |z_2\rangle \otimes \cdots \otimes |z_n\rangle. \tag{2.9}$$

Or we can even remove the commas to write

$$|z_1 z_2 \cdots z_n\rangle := |z_1\rangle \otimes |z_2\rangle \otimes \cdots \otimes |z_n\rangle. \tag{2.10}$$

All of these notations are equivalent.

Example 3: General Two Qubit State in Shorthand Notation

In our new shorthand notation, (2.5) becomes

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle. \tag{2.11}$$

How do we explicitly compute a tensor product? Suppose we have two arbitrary qubits

$$|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, \qquad |\phi\rangle = \begin{bmatrix} c \\ d \end{bmatrix}. \tag{2.12}$$

Then, the tensor product $|\psi\rangle \otimes |\phi\rangle$ evaluates to

$$|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix} a|\phi\rangle \\ b|\phi\rangle \end{bmatrix} = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}. \tag{2.13}$$

Since both qubits live in $\mathbb{C}^2$, the composite tensor product state lives in $\mathbb{C}^4$.

Exercise 13: Compute the tensor product $(|\psi\rangle \otimes |\phi\rangle) \otimes |\chi\rangle$ where $|\chi\rangle := [e\, f]^T$.

What about tensor products of basis states? It is easy to verify using (2.13) that

$$|0\rangle \otimes |0\rangle \equiv |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},\ |0\rangle \otimes |1\rangle \equiv |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},\ |1\rangle \otimes |0\rangle \equiv |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix},\ |1\rangle \otimes |1\rangle \equiv |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \tag{2.14}$$

Note that the binary value of the bit string in the ket denotes the position of the one in the basis vector. For example "00" in binary is 0 in decimal, and the entry with a one in the tensor product $|00\rangle$ is the 0th entry. Similarly for "01," "10," and "11." This binary to decimal bijective map leads to yet another notation. Namely, we can write $|00\rangle$ as $|0\rangle_2$. In the latter ket, the value 0 denotes a decimal value of 0, and the subscript 2 indicates that there are two bits in the former ket. Similarly, $|01\rangle$ becomes $|1\rangle_2$, $|10\rangle$ becomes $|2\rangle_2$, and $|11\rangle$ becomes $|3\rangle_2$. In contexts where it is absolutely clear, the subscript on the "decimal notation" kets may sometimes be dropped.

The tensor product has multiple properties which we'll cover in future sessions. For example, it is linear, associative, and distributive. However, it is NOT necessarily commutative.

Exercise 14: For $|\psi\rangle$ and $|\phi\rangle$ given in (2.12), verify by direct computation that $|\psi\rangle \otimes |\phi\rangle \neq |\phi\rangle \otimes |\psi\rangle$.

For now, we are just concerned with *how* states with multiple qubits work, for which are preliminary discussion of the tensor product will suffice.

We will mention several important *classes* of states that appear in quantum computing and quantum information science.

Definition 2.2 (Bipartite State). A **bipartite state** is a state on the composite space $H_{AB} = H_A \otimes H_B$ consisting of two "parts" (hence *bipartite*) H_A and H_B.

Definition 2.3 (Product State). A **product state** is a bipartite state on H_{AB} that can be written of the form $|\psi\rangle_A \otimes |\phi\rangle_B$ where $|\psi\rangle_A \in H_A$ and $|\phi\rangle_B \in H_B$.

Definition 2.4 (Separable State). A **separable state** is a convex combination of product states, i.e., a state that can be written as

$$\sum_{i,j} c_{i,j} |i\rangle_A \otimes |j\rangle_B \tag{2.15}$$

such that $\sum_{i,j} p_{i,j} = 1$.

Definition 2.5. An **entangled state** is any state that cannot be written as a separable state.

What's different about entangled states? Consider the following example.

Suppose Alice and Bob have qubits in Hilbert spaces H_A and H_B, respectively. If the composite state of their qubits were

$$|0\rangle_A \otimes |0\rangle_B, \tag{2.16}$$

then we would be correct in saying that Alice's qubit is in the state $|0\rangle$ and Bob's qubit is in the state $|0\rangle$. Similarly if the composite state of their qubits were

$$|1\rangle_A \otimes |1\rangle_B, \tag{2.17}$$

we would again correctly say that Alice's qubit is in the $|1\rangle$ state and Bob's qubit is in the $|1\rangle$ state.

Now, suppose that the composite state of their qubits were

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.18}$$

How would you describe Alice's qubit? Bob's? The answer is you cannot describe either of their qubits individually. The state of the entire composite system is specified, but neither component state can be determined. Alice's and Bob's qubits are *entangled*.

Entanglement plays a key role in the quantum teleportation algorithm and many other algorithms. Before we finally describe this algorithm, we first need to discuss how quantum gates can act on multiple qubits.

Example 4: Entanglement is Quantum Correlation.

What does "correlation" mean for two classical variables, x and y? It means that they are connected in some way. For example, if "x increases, then y increases" is an example of two variables that are (positively) correlated. Negative correlations are of the form "if x increases, y decreases." In either case, there is some form of connection between the two variables.

Entanglement is quantum correlation, that is, correlation between two quantum states. Consider the state given in (2.18), commonly known as a *Bell state* or *EPR pair* and denoted

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.19}$$

Suppose we measure the first qubit and obtain the zero outcome. What is the state immediately after measurement? We use Definition 2.1, specifically (2.3) and $M_0 = |0\rangle\langle 0|$ as a measurement on the *first* qubit only. Then, the state immediately after the measurement is

$$\frac{M_0|\Phi^+\rangle}{\sqrt{p(0)}} = \left(|0\rangle\langle 0| \otimes I\right)\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) = |0\rangle|0\rangle. \tag{2.20}$$

(We use $(|0\rangle\langle 0| \otimes I)$ because we only measure the *first* qubit and do nothing (or act with the identity operator) on the second qubit.)

Now look at what (2.20) tells us. If we measure the first qubit (Alice's qubit) to be in the zero state, then immediately after the measurement the second qubit (Bob's qubit) will also be in the zero state! The qubits are somehow *correlated* in a quantum sense that we call *entanglement*. If Bob measured his qubit after, he would always obtain 0 with 100% probability. Alice's and Bob's measurement statistics would be perfectly correlated.

Here's the interesting thing: Alice's measurement was *local*. It only acts on her qubit, she only touches her qubit, she never looks at Bob's qubit. However, despite this, the measurement somehow *non-locally* affects Bob's qubit. This is a demonstration of *non-locality* in quantum mechanics, which means that local actions can influence objects far away. (Imagine if Alice and Bob created an entangle pair of qubits then ran off to opposite sides of the world.)

Exercise 15: Suppose that Alice measured her qubit in (2.19) and got the one outcome. Similar to Example 2.2, show that the state immediately after the measurement is $|11\rangle$.

2.3 Multi-Qubit Gates

Now that we have multi-qubit states, we need to introduce multi-qubit gates. Just as single qubit gates determine the evolution of single qubits, multi-qubit gates determine the evolution of multiple qubits. Clear analogues exist in classical information processing. For example, the AND gate inputs two bits and outputs one bit. The output bit is one if both inputs are one and zero otherwise.

One of the most common two-qubit gates in quantum computing is the Controlled-NOT gate, commonly abbreviated CNOT. CNOT acts on two qubits, one of which is called *control* qubit, and the other called the *target* qubit. The CNOT gate flips the target qubit if the control qubit is in the one state. If the control qubit is not in the one state, then CNOT does nothing to the target qubit.

For example, suppose we have a two qubit state $|00\rangle$ that we want to perform $\text{CNOT}_{0,1}$ on. Here, the subscript means we want the first qubit (indexed 0) as the control and the second qubit (indexed 1) as the target. Since the first qubit is in the $|0\rangle$ state, nothing happens to the target qubit. The final state is thus $\text{CNOT}_{0,1}|00\rangle = |00\rangle$. Similarly, $\text{CNOT}_{0,1}|01\rangle = |01\rangle$ because the control qubit is still in the zero state.

The next two cases are $\text{CNOT}_{0,1}|10\rangle = |10\rangle$ and $\text{CNOT}_{0,1}|11\rangle = |10\rangle$. Here, in both cases we *flip* the target qubit because the control qubit is in the one state. In summary:

Definition 2.6 (Controlled-NOT Gate). The Controlled-NOT gate $\text{CNOT}_{0,1}$ (controlling on the first qubit with the second qubit as the target) has the following action on computational basis states:

$$\text{CNOT}_{0,1}|00\rangle = |00\rangle, \qquad \text{CNOT}_{0,1}|01\rangle = |01\rangle, \qquad \text{CNOT}_{0,1}|10\rangle = |11\rangle, \qquad \text{CNOT}_{0,1}|11\rangle = |10\rangle. \tag{2.21}$$

Exercise 16: Verify that a matrix representation for $\text{CNOT}_{0,1}$ is

$$\text{CNOT}_{0,1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.22}$$

in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Exercise 17: Prove, without using matrix multiplication, that $\text{CNOT}_{0,1}$ squares to the identity.

Exercise 18: Write down the action of $\text{CNOT}_{1,0}$ (control and target qubit reversed) on the computational basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Write out the matrix in this basis as well.

In future seminars, we'll see more two-qubit and multi-qubit gates. In general, m qubit gates are just unitary operators on m qubits. For the quantum teleportation algorithm, the CNOT gate is all we need to discuss.

2.4 The No-Cloning Theorem

We now have the ingredients—namely, multi-qubit states and multi-qubit gates—to prove the *no-cloning theorem*. Recall the problem of quantum teleportation: Alice has some unknown qubit that she wants to send to Bob. We already ruled out measuring the qubit to see what it was, for we saw that this would inherently modify the qubit. Why don't we just make a copy of it? Well, unfortunately this is what the no-cloning theorem forbids. Casually, it states that we cannot clone arbitrary quantum states by unitary evolution. A formal statement of the theorem is given below.

Theorem 2.2 (No-Cloning Theorem). Suppose U is a unitary operator that serves as a "quantum copy machine." That is, U is a two-qubit operator that copies (or *clones*) the first qubit into the second qubit

$$U|\psi\rangle|s\rangle = |\psi\rangle|\psi\rangle \tag{2.23}$$

where $|s\rangle$ is some arbitrary initial qubit. Then, U can *only* clone qubits parallel or orthogonal to $|\psi\rangle$.

Proof. The proof of this theorem is actually rather simple. Since the theorem is about the ability of U to clone other states, let's right down (2.23) for some other arbitrary state $|\phi\rangle$,

$$U|\phi\rangle|s\rangle = |\phi\rangle|\phi\rangle. \tag{2.24}$$

Now we're going to "compare" (2.23) and (2.24) in some sense by taking an inner product between them. First, if we consider the left-hand sides of these equations, then we have

$$\langle\phi| \otimes \langle s|U^\dagger U|\psi\rangle \otimes |s\rangle = \langle\phi|\psi\rangle\langle s|s\rangle = \langle\phi|\psi\rangle \tag{2.25}$$

where we have used that U is unitary and that inner products "distribute" across tensor products. If we consider the right-hand sides of (2.23) and (2.24) when taking inner products, then we have

$$(\langle\phi| \otimes \langle\phi|)\,(|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2. \tag{2.26}$$

But of course the expressions (2.25) and (2.26) must be equal, i.e.

$$\langle\phi|\psi\rangle =< \phi|\psi\rangle^2. \tag{2.27}$$

This equation is of the form $x^2 = x$ (where $x \equiv \langle\phi|\psi\rangle$) which has only two solutions: $x = 0$ or $x = 1$. If $x = 1$, then $|\phi\rangle$ and $|\psi\rangle$ are parallel. If $x = 0$, then $|\phi\rangle$ and $|\psi\rangle$ are orthogonal. Thus, U can only possibly clone qubits parallel or orthogonal to $|psi\rangle$, which completes the proof. ☐

So quantum information forbids Alice explicitly reading her qubit and sending that information to Bob, and also forbids Alice cloning her qubit and sending the clone to Bob. (This would not work in general, as we have seen, and we have no information about the qubit she wants to send.) There is still a way for Alice to send her unknown qubit to Bob via the interesting result of *quantum teleportation*.

2.5 Quantum Teleportation Algorithm

Quantum teleportation involves an intermediary qubit between Alice and Bob. It relies on quantum entanglement, specifically creating an EPR pair that is "shared" between Alice and Bob. The circuit for the teleportation algorithm is shown below.

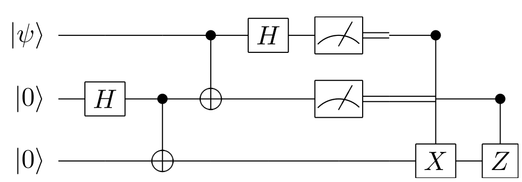

Figure 2.1: Circuit diagram for the quantum teleportation algorithm.

We assume the the first qubit (the top qubit in the diagram), which belongs to Alice, starts out in the $|\psi\rangle$ state, since this is what the quantum teleportation algorithm assumes. The bottom two qubits belong to Bob. The first thing Bob does is create an EPR pair (2.19) with his two qubits, doing a Hadamard on one then performing a controlled not gate.

To see that this circuit indeed creates an EPR pair, note that we start out with both qubits in the $|0\rangle\otimes|0\rangle$ state. We then perform a Hadamard gate on the first qubit and do nothing on the second qubit. Thus, the overall multi-qubit gate that we perform is $H \otimes I$. The action of this gate on the $|0\rangle \otimes |0\rangle$ state is

$$(H \otimes I)|0\rangle \otimes |0\rangle = H|0\rangle \otimes I|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \tag{2.28}$$

This is *almost* an EPR pair. To make it exactly an EPR pair, we can perform a CNOT, controlling on the first qubit. Doing so yields

$$\mathrm{CNOT}_{0,1}\frac{1}{\sqrt{2}}\left(|00\rangle+|10\rangle\right)=\frac{1}{\sqrt{2}}\left(\mathrm{CNOT}_{0,1}|00\rangle+\mathrm{CNOT}_{0,1}|10\rangle\right)=\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right) \tag{2.29}$$

In the first step, we used linearity, and in the second step we used the definition of the CNOT gate (Definition 2.21).

We now have Bob's qubits in an EPR pair. The next step is to have Alice perform a CNOT gate between her qubit and one of Bob's qubits. (This is the "shared" qubit part that we mentioned before.) Note that the state of the entire system (Alice + Bob's qubits) is

$$\frac{1}{\sqrt{2}}|\psi\rangle\otimes\left(|00\rangle+|11\rangle\right). \tag{2.30}$$

How can we perform a CNOT gate with arbitrary state $|\psi\rangle$? The key is to express it in terms of the computational basis states

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \tag{2.31}$$

for some unknown coefficients $\alpha,\beta\in\mathbb{C}$. If we distribute this term into the entire state (2.30), we get four terms describing the whole state

$$\frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle\right) \tag{2.32}$$

This expression enables us to easily perform a CNOT gate between the first and second qubits. Doing so, we obtain the state

$$\frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|011\rangle+\beta|110\rangle+\beta|101\rangle\right) \tag{2.33}$$

We then perform a Hadamard gate on the first qubit to get

$$|\Psi\rangle:=\frac{1}{2}\left(\alpha|000\rangle+\alpha|100\rangle+\alpha|011\rangle+\alpha|111\rangle+\beta|010\rangle-\beta|110\rangle-\beta|101\rangle+\beta|001\rangle\right). \tag{2.34}$$

These are all the gate operations that we need to perform before we measure. To get a better idea of the possible outcomes we can get when we measure, we can group terms containing the same state for the first two terms. There are four possibilities for the first two qubits, namely $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Grouping these terms together, we can rewrite the state as

$$|\Psi\rangle=\frac{1}{2}\left(|00\rangle(\alpha|0\rangle+\beta|1\rangle+|01\rangle(\alpha|1\rangle+\beta|0\rangle+|10\rangle(\alpha|0\rangle-\beta|1\rangle+|11\rangle(\alpha|1\rangle-\beta|0\rangle\right). \tag{2.35}$$

Exercise 19: Expand each term in (2.35) to get the same state in (2.34), thus verifying they are equal.

Now Alice measures her two qubits (the first two qubits). Suppose she gets the $|00\rangle$ outcome. Then, Bob's qubit is in the state $\alpha|0\rangle+\beta|1\rangle$, which is $|\psi\rangle$ exactly. In this case, we are done, and Alice's unknown qubit $|\psi\rangle$ has been teleported to Bob.

This is not the only possible measurement outcome Alice could obtain, however. Suppose instead she measures $|01\rangle$. By looking at (2.35), we see that Bob's qubit in this case would be $\alpha|1\rangle+\beta|0\rangle$. This is *almost* $|\psi\rangle$, but the amplitudes are flipped. How can we get $|\psi\rangle$ exactly from this state? We can perform a NOT gate $X(\alpha|1\rangle+\beta|0\rangle)=\alpha|0\rangle+\beta|1\rangle=|\psi\rangle$. If Bob performs a NOT gate on his qubit in this case, then he again obtains $|\psi\rangle$ exactly.

The other two measurement cases can easily be worked out as well.

Exercise 20: If Alice measures $|10\rangle$, prove that Bob's qubit is in the state $\alpha|0\rangle-\beta|1\rangle$. Further, prove that he can obtain $|\psi\rangle$ by performing a Pauli-Z gate on his qubit. That is, $Z(\alpha|0\rangle-\beta|1\rangle)=|\psi\rangle:=\alpha|0\rangle+\beta|1\rangle$.

Exercise 21: If Alice measures $|11\rangle$, prove that Bob's qubit is in the state $\alpha|1\rangle - \beta|0\rangle$. Further, prove that he can obtain $|\psi\rangle$ by performing a NOT gate and then performing Pauli-Z gate on his qubit. That is, $ZX(\alpha|1\rangle - \beta|0\rangle) = |\psi\rangle := \alpha|0\rangle + \beta|1\rangle$. Also prove that he can first do Z and then do X to still obtain $|\psi\rangle$. (In general Z and X anticommute, i.e. $ZX = -XZ$, which you may want to prove by direct computation.)

Thus, in all four measurement cases, Bob is able to obtain exactly Alice's unknown qubit $|\psi\rangle$ without either knowing what the actual state is. For clarity, we enumerate all measurement possibilities in the table below.

Alice measures:	**Bob performs:**
$\|00\rangle$	I
$\|01\rangle$	X
$\|10\rangle$	Z
$\|11\rangle$	ZX

Table 2.1: All possible measurement outcomes of the quantum teleportation algorithm.

Note that the controlled-gates after the measurements on Alice's qubits in Figure 2.1 perform exactly these operations. After the measurement, we have classical information, which we represent in circuit diagrams with two lines (instead of one line for qubits). The controlled-X and controlled-Z are thus conditional on these measurement outcomes. If the first qubit comes out to be a zero, then we *do not* perform an X gate on Bob's qubit. If the first qubit does come out to be zero, then we do perform an X gate. Similarly for the controlled-Z in the standard sense of controlled operations.

Note that there must be some form of (classical) communication between Alice and Bob after Alice makes measurements and before Bob performs operations. If Alice measures $|00\rangle$, she has to tell Bob "I measured $|00\rangle$," at which point Bob knows to do nothing. Similarly for the other three possibilities. Without this communication, Bob would have no idea what to do.

In this sense, it is important to emphasize that *no information, classical or quantum, is really being "teleported" here,* despite the name of the algorithm. Alice's classical "communication" is of course limited by the speed of light. Although "teleport" may imply instantaneous information transfer, that is not what is happening here. It is interesting nonetheless that neither Alice nor Bob know anything about the actual state of the qubit $|\psi\rangle$ being teleported. We've shown that $|\psi\rangle$ could be any arbitrary qubit and the teleportation algorithm works just fine.

Example 5: Quantum Teleportation with a Particular Qubit

In the teleportation circuit shown in Figure 2.1, we assumed $|\psi\rangle$ was already input to the circuit. In this setting, we think of Alice in a lab setting performing some experiment that produces an unknown qubit. Practically with quantum circuits, we always have control over what states we have in our algorithms. Let's suppose we wanted to construct an explicit circuit to teleport a given qubit, just as an illustrative example. Let's arbitrarily pick Alice's qubit to be $|1\rangle$.

Conventionally, all qubits start in the ground state $|0\rangle$ at the beginning of a quantum algorithm. So we need some way of preparing $|1\rangle$ from $|0\rangle$. This can be done with a NOT gate X.

The entire quantum teleportation circuit for this particular example thus takes the following form shown in Figure 2.2. An example sending arbitrary states can be found at this link on the visual quantum circuit simulator Quirk by Craig Gidney. [citation needed]

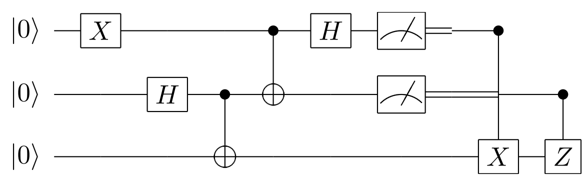

Figure 2.2: Quantum teleportation algorithm for the particular qubit $|1\rangle$.