Lecture 10, Thurs Feb 16: Teleportation, Entanglement Swapping, GHZ, Monogamy

Next let's see...

Quantum Teleportation

which is a result from 1991 that came as a great surprise. Science journalists still love it given its irresistible name. In this lecture we'll see what it can and can't do.

Firstly, what does teleportation mean?

You might think it implies sending qubits instantaneously over vast distances, but that can't be done, as it violates the causal structure of the universe. So we're only going to send qubits at the speed of light, no faster. Of course, there are other ways to move qubits at the speed of light or slower, like just picking them up and moving them, or putting them on a bus! (It doesn't sound as sexy that way.)

OK, but what if you only had a phone line, or a standard Internet connection? That would let you send classical bits, but not qubits. With teleportation, though, we'll achieve something surprising. We'll show:

It is possible for Alice and Bob to use pre-shared entanglement plus classical communication to perfectly transmit a qubit.

The inequality here is almost the converse of the one for superdense coding:

$$1 \text{ ebit} + 2 \text{ bits} \geq 1 \text{ qubit}$$

Which is to say, you need one pair of entangled qubits plus two classical bits in order to transmit one qubit. (This can also be shown to be optimal.)

We'll give a more in-depth explanation in the next lecture, but the gist of it is:

Alice has, say, a single qubit, $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. She also shares a Bell pair with Bob.

Alice applies some transformation to $|\Psi\rangle$ that entangles it with her half of the Bell pair. She then measures her qubits.

Alice tells Bob the measurement outcomes over the phone.

Bob applies some transformations (to his qubit of the entangled pair), based on what he hears from Alice.

"Magically," Bob now has $|\Psi\rangle$
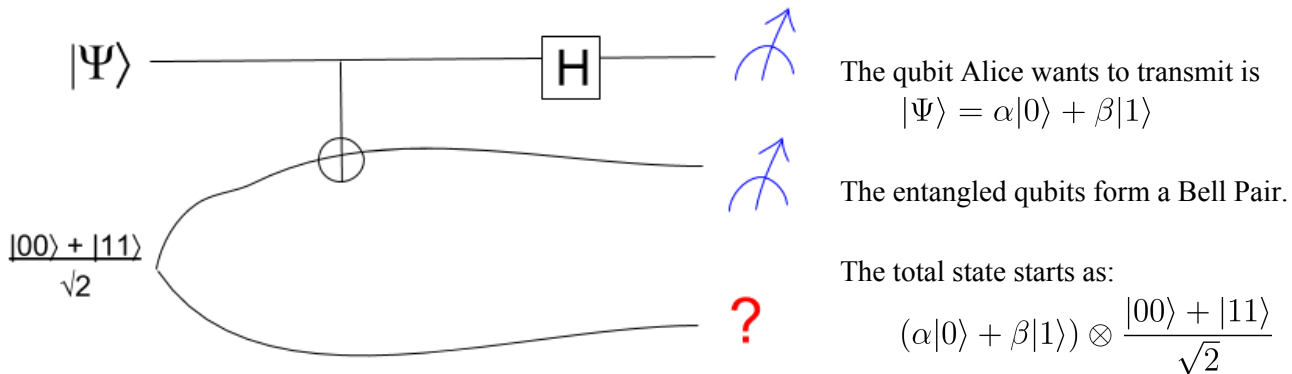
At the end, will Alice also have $|\Psi\rangle$?

No. A logical consequence of the No Cloning Theorem is that there can only be one copy of the qubit.

Could we hope for a similar protocol *without* sending classical information?

No, because of the No-Communication Theorem.

So let's say Alice wants to get a qubit over to Bob, *without* using a quantum communication channel, but *with* a classical channel together with preshared entanglement. How should Alice go about this?

Once the question is posed, you can play around with different combinations of operations, and you'd eventually discover that what works is this:

The qubit Alice wants to transmit is
$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

The entangled qubits form a Bell Pair.

The total state starts as:
$$(\alpha|0\rangle + \beta|1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Then Alice applies a cNOT gate (with $|\Psi\rangle$ as the control, and her half of the Bell pair as the target):
$$\frac{1}{\sqrt{2}}[\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle]$$

Alice then Hadamards her $|\Psi\rangle$ qubit:
$$\frac{1}{2}[\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle]$$

Finally, Alice measures both of her qubits in the $\{|0\rangle, |1\rangle\}$ basis.
This leads to four possible outcomes:

If Alice Sees	00	01	10	11
Then Bob's qubit is	$\alpha|0\rangle + \beta|1\rangle$	$\alpha|1\rangle + \beta|0\rangle$	$\alpha|0\rangle - \beta|1\rangle$	$\alpha|1\rangle - \beta|0\rangle$

We're deducing information about by Bob's state by using the partial measurement rule. E.g., if Alice sees 00, then we narrow down the state of the entire system to the possibilities that fit, namely $|000\rangle$ and $|001\rangle$.

What is Bob's state, if he knows that Alice measured, but doesn't know the measurement outcome?
It's an equal mixture of all four possibilities, which is just the Maximally Mixed State.
This makes sense given the No-Communication Theorem! Until Alice sends information over, Bob's qubit can't possibly depend on $|\Psi\rangle$.

Next, Alice tells Bob her measurement results via a classical channel. And Bob uses the information to "correct" his qubit to $|\Psi\rangle$.

If the first bit sent by Alice is 1, then Bob applies $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

If the second bit sent by Alice is 1, then Bob applies $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

These transformations will bring Bob's qubit to the state $\alpha|0\rangle + \beta|1\rangle = |\Psi\rangle$.
That means they've successfully transmitted a qubit without a quantum channel!

This protocol never assumed that Alice knew what was $|\Psi\rangle$.

For this protocol to work, Alice had to measure her **syndrome** bits. These measurements were destructive (since we can't ensure that they'll be made in a basis orthonormal to $|\Psi\rangle$, and thus Alice doesn't have $|\Psi\rangle$ at the end. Alice and Bob also "use up" their Bell pair in the process of teleporting $|\Psi\rangle$.

Something to think about: Where is $|\Psi\rangle$ after Alice's measurement, but before Bob does his operations?

How do people come up with this stuff? I can't picture how anyone trying to solve this problem would even begin their search…
Well it's worth pointing out that quantum mechanics was discovered in 1926 and that quantum teleportation was only discovered in the 90's. These sorts of protocols *can* be hard to find. Sometimes someone tries to prove that something is impossible, and in doing so eventually figures out a way to get it done...

Aren't we fundamentally sending infinitely more information than two classical bits if we've sent over enough information to perfectly describe an arbitrary qubit, since the qubit's amplitudes could be arbitrary complex numbers?
In some sense, but at the end of the day, Bob only really obtains the information that he can measure, which is significantly less. Amplitudes may "exist" physically, but they're different from other physical quantities like length, in that they seem to act a lot more like probabilities.
Like, there's a state $\alpha|0\rangle + \beta|1\rangle$, of a single qubit, such that β is a binary encoding of the complete works of Shakespeare—the rules of quantum mechanics don't put a limit on the amount of information that it takes to specify an amplitude. With that said, we could also encode the complete works of Shakespeare into the probability that a classical coin lands heads! In both cases, the works of Shakespeare wouldn't actually be retrievable by measuring the system.

If we can teleport one qubit, the next question we may want to ask is:

Can we go further? What would it take to teleport an arbitrary quantum state, say of *n* qubits?

To answer this question, let's notice that nothing said that a qubit that's teleported has to be unentangled with the rest of the world.

You could run the protocol and have $|\Psi\rangle$ be half of another Bell pair. That would entangle the fourth qubit to Bob's qubit (you can check this via calculation). That's not a particularly interesting operation, since it lands you where you started, with one qubit of entanglement between Alice and Bob, but it does have an interesting implication.
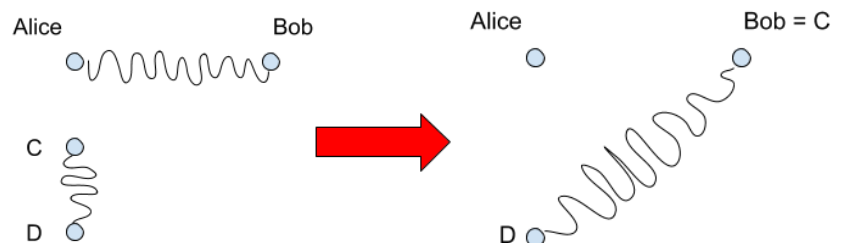
It suggests that it should be possible to teleport an arbitrary n-qubit entangled state, by simply teleporting the qubits one at a time, thus using n ebits of preshared entanglement. And indeed it's not hard to check that that works.

One further consequence of this is that two qubits don't need to interact directly to become entangled.
  In some sense, we already knew that:
  Consider for example the following circuit.

Swap Gate
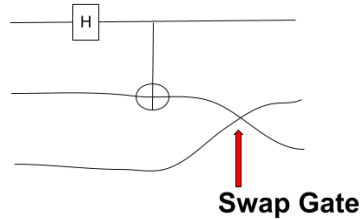
Here the first and third end up entangled, even though there's never "direct" contact between them: the second qubit serves as an intermediary.

However, teleportation leads to something
much more surprising than this, called...
Entanglement Swapping

If Alice has two entangled qubits, and also two Bell pairs shared with Bob, she can teleport both of her qubits to Bob, whereupon they'll be entangled on Bob's end … even though the two qubits on Bob's end, which are now entangled, were never in causal contact with one another!

This process has been used in real experiments, such as the recent "loophole-free Bell tests," about which we'll learn more later in the course.

By the way, quantum teleportation itself has been demonstrated experimentally many times.

A few more comments on the nature of entanglement:

We've seen the Bell pair, and what it's good for. There's a 3-qubit analogue of it called the **GHZ state**: $\frac{|000\rangle + |111\rangle}{\sqrt{2}}$. We'll see applications of the GHZ state later in the course, but for now we'll use it to illustrate an interesting conceptual point.
  Let's say that Alice, Bob, and Charlie hold random bits, which are either all 0 or all 1 (so, they're classically correlated). If all three of them get together, they can see that their bits are correlated, and *the same is true if only two of them are together*.
  But now suppose the three players share a GHZ state. With all three of them, they can see that the state is entangled, but what if Charlie is gone? Can Alice and Bob see that they're entangled with each other?
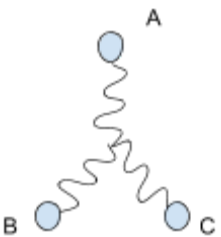
No. To see this, observe that by the No-Communication Theorem, Charlie could've measured without Alice and Bob knowing. But if he did, then Alice and Bob would clearly have classical correlation only: either both 0's (if Charlie got the measurement outcome 0) or both 1 (if Charlie got 1). From this it follows that Alice and Bob have only classical correlation *regardless of whether Charlie measured or not*.

A different way to see this is to look at the density matrix of the state shared by Alice and Bob:

$$\rho_{AB} = \begin{bmatrix} \frac{1}{2} & & & \\ & & & \\ & & & \\ & & & \frac{1}{2} \end{bmatrix} \qquad \text{(all blank entries are 0)}$$

And notice that this is different than the density matrix of a Bell pair shared by Alice and Bob

$$\rho_{AB} = \begin{bmatrix} \frac{1}{2} & & \frac{1}{2} & \\ & & & \\ \frac{1}{2} & & \frac{1}{2} & \\ & & & \end{bmatrix} = |\Psi\rangle\langle\Psi|$$

Where $|\Psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$

This is one illustration of a general principle called…

The Monogamy of Entanglement

Simply put, this means that if Alice has a qubit that is maximally entangled with Bob, then that qubit can't also be maximally entangled with Charlie.
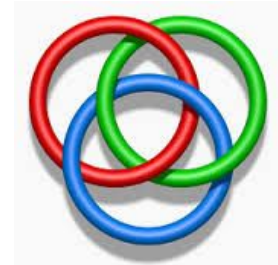
With GHZ, you can only see the entanglement if you have all three qubits together. This is sometimes analogized to the Borromean Rings (right), an arrangement of three rings with the property that all three are linked together, without any two of them being linked together.

There are other 3-qubit states which aren't like that…

In the W state, $\frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$, there's *some* entanglement between Alice and Bob, and there's *some* entanglement between Alice and Charlie, but neither pair is *maximally entangled*.

As for how you quantify entanglement … well, that will be the subject of the next lecture!