Lecture 9: Tues Feb 14: Superdense Coding

OK, now on to some new stuff!

Superdense Coding

is the first protocol we'll see that requires entanglement. Basic information theory (Shannon) tells us that "by sending n bits, you can't communicate more than n bits of information."

Now, by contrast, we'll see how Alice can send Bob *two* classical bits by sending him only *one* qubit, though there is a catch: Alice and Bob must share some entanglement ahead of time.

In the scenario with no prior entanglement, Alice can't send more than one bit per qubit—a fundamental result known as *Holevo's Theorem*.

We're not going to prove Holevo's Theorem here, but the intuition is pretty simple: if Alice sends $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob, he can only measure it once in some basis and then the rest of the information in $|\Psi\rangle$ is lost.

Instead, let's suppose that Alice and Bob share a Bell pair in advance: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

We claim that Alice can manipulate her half, then send her half to Bob, and then Bob can measure both qubits and get two bits of information from Alice.

The key is to realize that Alice can get three different states, all of them orthogonal to the original Bell pair and to each other, by applying the following gates to her qubit:

- NOT $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ which gives us $\frac{|01\rangle + |10\rangle}{\sqrt{2}}$
- A phase change $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ which gives us $\frac{|00\rangle - |11\rangle}{\sqrt{2}}$
- And applying both NOT and a phase change, which gives us $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$

These four states form an orthogonal basis.

So suppose Alice wants to transmit two bits X, and Y:

If $X = 1$, she applies the NOT gate.
If $Y = 1$, she applies a phase gate.
Then she sends her qubit to Bob.

We can derive her encoding matrix as: $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{bmatrix}$

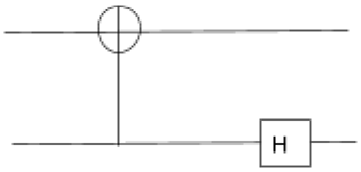
Which makes sense, because each column corresponds to one of the four states we listed above.

(e.g. the second column corresponds to $\dfrac{|00\rangle - |11\rangle}{\sqrt{2}}$)

For Bob to decode this transformation, he'll want to use the inverse transformation:

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

Which corresponds to the circuit:



cNOT (2nd controls 1st)
then Hadamard on the 2nd qubit

So, Alice transforms the Bell pair into one of the four orthogonal states above, then Bob decodes that two-qubit state into one of the four possible combinations of $|0\rangle$ and $|1\rangle$, corresponding to the original bits X and Y.

For example:

if Bob receives $\dfrac{|01\rangle - |10\rangle}{\sqrt{2}}$, applying cNOT gets him $|1\rangle \otimes |-\rangle$, and Hadamard gets him $|1\rangle \otimes |1\rangle$.

if Bob receives $\dfrac{|00\rangle - |11\rangle}{\sqrt{2}}$, applying cNOT gets him $|0\rangle \otimes |+\rangle$, and Hadamard gets him $|0\rangle \otimes |1\rangle$.

Naturally, we could ask: if Alice and Bob had even more pre-shared entanglement, could Alice send an arbitrarily large amount of information by transmitting only one qubit?

There's a theorem that says: No.

It turns out that for every qubit, and any amount of entangled qubits (ebits), you can send two bits of classical information, but no more. I.e., we can write the inequality:

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

but **not**

$$1 \text{ qubit} + \text{ebits} \geq 3 \text{ bits}$$

As far as quantum speed-ups go, a factor of two isn't particularly impressive, but it is pretty cool that it challenges the most basic rules of information theory established by Shannon himself.