Tues Feb 14

To review: We've seen 3 different types of states in play:

- Basis States
  - exist in a computational basis $|i\rangle$
- Pure States
  - superpositions of basis states $|\Psi\rangle = \Sigma\ \alpha_i|i\rangle$
- Mixed States
  - classical probabilities over pure states $\rho = \Sigma\ \rho_i|\Psi_i\rangle\langle\Psi_i|$

Which represents the actual physical reality: pure or mixed states?

It's complicated. Sometimes we use density matrices to represent our probabilistic ignorance of a state, but other times (i.e. entangled states) they represent the maximal truth that exists of the state. We'll generally just focus on what these representations are useful for.

Wiesner's Scheme, as we've seen it, requires the bank to hold a lot of information. The paper (BBBW 82) circumvents this by basically saying: Let f be a pseudorandom function, so that for any state S_k the bank can compute $f(S_k)$.
Why is this secure?

We use a reduction argument. Suppose that the counterfeiter can copy money by some means. What does that say about f_k? If it is pseudorandom, then f_k is distinguishable from a random function, so it's not very good at being pseudorandom.

Superdense Coding

is the first protocol we'll see that involves entanglement. Basic information theory (Shannon) tells us that "with n bits you can't send more than n bits of information."

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

In the scenario with no prior entanglement, you can't send more than one bit per qubit.

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: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

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

The key is to realize that Alice can get a state orthogonal to the Bell Pair by applying the following gates to her bit:

- NOT $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which gives us $\frac{|01\rangle + |10\rangle}{\sqrt{2}}$

- A phase change (1 0) which gives us $\frac{|00\rangle - |11\rangle}{\sqrt{2}}$
  (0 -1)
- And applying both NOT and a phase change $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$

More specifically, any pair of these four states is orthogonal.

Say Alice wants to transmit two bits X, and Y:

If X = 1, she applies the NOT gate.

If Y = 1, she applies a phase change

Then she sends her bit to Bob.

We can derive her encoding matrix as:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix}$$

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

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

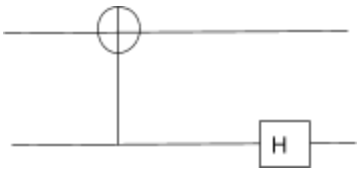
For Bob to decode this transformation, he'll want to use its matrix transform:

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

Which corresponds to the gates:

cNOT (2nd controls 1st)

then Hadamard (2nd qubit)



The idea is that Alice transforms the Bell Pair into one of the four entangled states above, then Bob decodes that two-qubit state into one of the four possible combinations of $|0\rangle$ and $|1\rangle$ which correspond to the variables X and Y.

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

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

Naturally, we may want to ask: if Alice and Bob had even more preshared entanglement, could Alice send an arbitrarily large amount of information through one qubit?

There's a theorem which answers: No.

It turns out that for every qubit, and any amount of entangled qubits (ebits), you can send two bits of classical information. We show this through the inequality:

1 qubit + ebits $\geq$ 2 bits

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

Quantum Teleportation

is a result from 1991 that came as a great surprise. You'll still see it in the news sometimes given its irresistable name. In this lecture we'll over what it can and can't do.

Firstly, what does teleportation mean?

You might think it implies sending qubits instantaneously over distances, but that can't be done (as it violates the causal structure of the universe). "Moving something", or "Putting it on a bus" are less-sexy, but more apt ways of describing it. Fundamentally it means:

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

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

1 ebit + 2 bits $\geq$ 1 qubit

Which is to say, you need one pair of entangled qubits plus two classical bits in order to transmit one qubit.

A more in depth explanation is given in the next lecture, but the gist of it is:
Alice has $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
Alice applies some transformation to $|\Psi\rangle$, then measure it.
Alice tells Bob some classical information on the phone.
Bob does some transformations (to his qubit of the entangled pair).
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.