QI Lecture 12

Quantum Communication

Classical Teleportation

To understand the philosophy of quantum teleportation, we'll first consider "classical teleportation".[1] Say you have three coins, A, B, and C, all of which are covered. We'll call the side of the coin that's up, heads or tails, "the face". The only thing you know about these coins is that B and C have the same face. They're not entangled, but they are correlated.

The trick to classical teleportation is to transfer the face of coin A onto coin C, without ever finding out anything about the face of any of the three coins. The idea behind the operation is illustrated in figure 1: if A and B have the same face, leave C alone, and if A and B are different, flip C over.

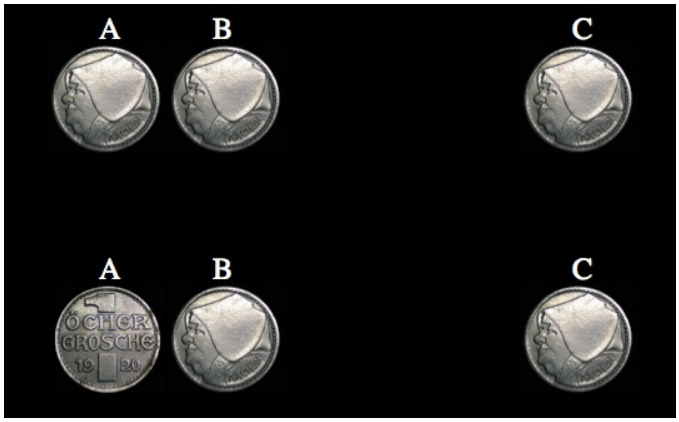

Figure 1: If B and C are always the same, then by comparing A and B we can determine what to do to C to make it the same as A.

To do this procedure, we start with B and C exposed and arrange them to have the same face. Then we hide them[2] and flip them together[3], so that they'll have the same, unknown, face.

[1] This is the only place you'll ever hear someone talk about "classical teleportation".

[2] For example, by placing them in a folded sheet of paper.

[3] For example, by holding them and turning them over until we've lost track of how many times we've turned them.

We then take A, also with an unknown face, and flip it together with B. Although this flipping destroys the face information of both coins, it maintains their same-or-different state.

Finally, expose A and B while keeping C hidden. If they are the same, then leave C alone, and if they are different, flip C. C will now have the same face A did at the beginning, and yet at no time did we gain any information about the original face of any coin. Even more profound, the probability distribution on A has been transferred to C; if there was a 90% chance that A was heads, the same is now true of C.

Quantum Teleportation

Quantum teleportation works very much the same as classical teleportation. As we saw in the examples above, a direct measurement of an entangled state "breaks the entanglement". Given $|\Psi_+\rangle$, if Alice sees the $|1\rangle$ state, then Bob's qubit is in the $|1\rangle$ as well,[4] so their collective state is $|1\rangle_a|1\rangle_b$ and not $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. So, like in the classical teleportation example, we need a way to transfer one qubit onto another without actually observing them.

The trick to this is shown in figure 2. Qubits B and C start entangled, as possibly very far apart. Qubit A is near qubit B and we'd like to induce C to have the same state.

Because B and C are "very far apart" we're forced to use LOCC,[5] "local operators and classical communication". Since A and B are in the same place we can apply any operator we like to the two of them, but any operations on C must be single-qubit operations.

Here's the teleportation algorithm.

- 1) Prepare the state $|\Psi_+\rangle_{bc}$, bring A and B together and move B and C apart.
- 2) Alice measure qubits A and B in the Bell basis, $|B_{jk}\rangle$.
- 3) Alice sends the results, j, k, to Bob over a classical channel.
- 4) Bob $Z^j X^k$ on C, dependent on the j, k he received from Alice.
- 5) C is now in the state that A was in.

We can see how teleportation works by following the states through the circuit. Qubit A, which we wish to teleport to C, starts in an arbitrary state, $|\psi\rangle_a = \alpha|0\rangle_a + \beta|1\rangle_a$. B and C start in $|\Psi_+\rangle_{bc} = \frac{|0\rangle_b|0\rangle_c+|1\rangle_b|1\rangle_c}{\sqrt{2}}$. Expanding $|\psi\rangle_a|\Psi_+\rangle_{bc} = (\alpha|0\rangle_a + \beta|1\rangle_a)\left(\frac{|0\rangle_b|0\rangle_c+|1\rangle_b|1\rangle_c}{\sqrt{2}}\right)$ we can write the initial state in the computational basis.

[4] A more delicate way to say this is that Alice and Bob will always find that their measurements are consistent with each other when they meet up to compare notes later. To say that Alice's measurement has any direct impact on Bob's state is false.

[5] More on this later.

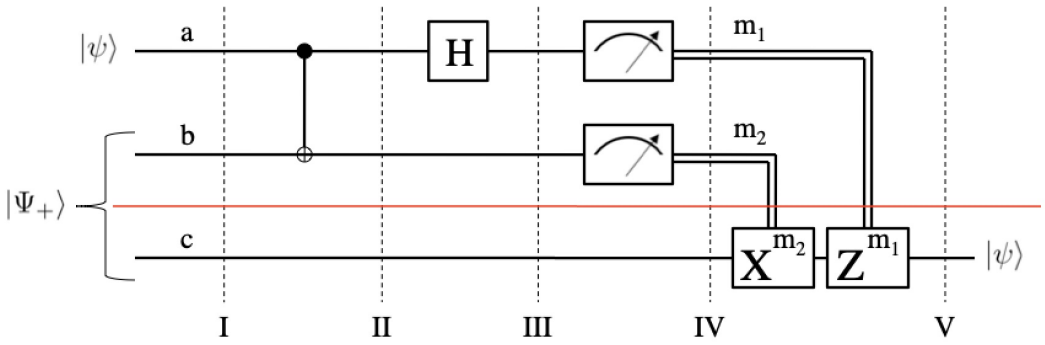

Figure 2: The red line signifies that, typically, the two parts of the entangled state are physically moved apart so that no quantum operation can be performed between the two. Double lines represent a classical channel (bits not qubits). The CNOT, Hadamard, and measurements on qubits a and b amount to a single measurement in the Bell Basis. That result is sent through a classical channel (like a phone call) to whomever is in charge of qubit c, who executes operations on c based on the result.

$$I: \quad \frac{\alpha}{\sqrt{2}}|0\rangle_a|0\rangle_b|0\rangle_c + \frac{\alpha}{\sqrt{2}}|0\rangle_a|1\rangle_b|1\rangle_c + \frac{\beta}{\sqrt{2}}|1\rangle_a|0\rangle_b|0\rangle_c + \frac{\beta}{\sqrt{2}}|1\rangle_a|1\rangle_b|1\rangle_c$$

We can follow the states through the circuit, but the quickest way to understand what this circuit is doing is to notice that everything above the red line in figure 2 is just a measurement on A and B in the Bell basis. So, we'll rewrite the first two qubits in the initial state in the Bell basis. Here's a chart to make it easy to go back and forth:

$$\left.\begin{aligned} |B_{00}\rangle &= \tfrac{|00\rangle+|11\rangle}{\sqrt{2}} \\ |B_{01}\rangle &= \tfrac{|01\rangle+|10\rangle}{\sqrt{2}} \\ |B_{10}\rangle &= \tfrac{|00\rangle-|11\rangle}{\sqrt{2}} \\ |B_{11}\rangle &= \tfrac{|01\rangle-|10\rangle}{\sqrt{2}} \end{aligned}\right\} \leftrightarrow \left\{\begin{aligned} |00\rangle &= \tfrac{|B_{00}\rangle+|B_{10}\rangle}{\sqrt{2}} \\ |01\rangle &= \tfrac{|B_{01}\rangle+|B_{11}\rangle}{\sqrt{2}} \\ |10\rangle &= \tfrac{|B_{01}\rangle-|B_{11}\rangle}{\sqrt{2}} \\ |11\rangle &= \tfrac{|B_{00}\rangle-|B_{10}\rangle}{\sqrt{2}} \end{aligned}\right.$$

$$\begin{aligned} & \tfrac{\alpha}{\sqrt{2}}|0\rangle_a|0\rangle_b|0\rangle_c + \tfrac{\alpha}{\sqrt{2}}|0\rangle_a|1\rangle_b|1\rangle_c + \tfrac{\beta}{\sqrt{2}}|1\rangle_a|0\rangle_b|0\rangle_c + \tfrac{\beta}{\sqrt{2}}|1\rangle_a|1\rangle_b|1\rangle_c \\ = \; & \tfrac{\alpha}{\sqrt{2}}\left(\tfrac{|B_{00}\rangle_{ab}+|B_{10}\rangle_{ab}}{\sqrt{2}}\right)|0\rangle_c + \tfrac{\alpha}{\sqrt{2}}\left(\tfrac{|B_{01}\rangle_{ab}+|B_{11}\rangle_{ab}}{\sqrt{2}}\right)|1\rangle_c + \tfrac{\beta}{\sqrt{2}}\left(\tfrac{|B_{01}\rangle_{ab}-|B_{11}\rangle_{ab}}{\sqrt{2}}\right)|0\rangle_c + \tfrac{\beta}{\sqrt{2}}\left(\tfrac{|B_{00}\rangle_{ab}-|B_{10}\rangle_{ab}}{\sqrt{2}}\right)|1\rangle_c \\ = \; & \tfrac{\alpha}{2}\left(|B_{00}\rangle_{ab}+|B_{10}\rangle_{ab}\right)|0\rangle_c + \tfrac{\alpha}{2}\left(|B_{01}\rangle_{ab}+|B_{11}\rangle_{ab}\right)|1\rangle_c + \tfrac{\beta}{2}\left(|B_{01}\rangle_{ab}-|B_{11}\rangle_{ab}\right)|0\rangle_c + \tfrac{\beta}{2}\left(|B_{00}\rangle_{ab}-|B_{10}\rangle_{ab}\right)|1\rangle_c \\ = \; & \tfrac{1}{2}|B_{00}\rangle_{ab}\left[\alpha|0\rangle_c+\beta|1\rangle_c\right] + \tfrac{1}{2}|B_{01}\rangle_{ab}\left[\beta|0\rangle_c+\alpha|1\rangle_c\right] + \tfrac{1}{2}|B_{10}\rangle_{ab}\left[\alpha|0\rangle_c-\beta|1\rangle_c\right] + \tfrac{1}{2}|B_{11}\rangle_{ab}\left[-\beta|0\rangle_c+\alpha|1\rangle_c\right] \end{aligned}$$

When the first two qubits are measured in the Bell basis, the result $|B_{jk}\rangle$, dictates what will be done to qubit C. After Bob receives j and k, he applies $Z^j X^k$ to his qubit (e.g., for $j = 0$, $k = 1$ he applies $Z^0 X^1 = IX = X$).

$$\begin{cases} |B_{jk}\rangle & & X^k & & Z^j & \\ |B_{00}\rangle: & \alpha|0\rangle_c + \beta|1\rangle_c & \xrightarrow{I} & \alpha|0\rangle_c + \beta|1\rangle_c & \xrightarrow{I} & \alpha|0\rangle_c + \beta|1\rangle_c \\ |B_{01}\rangle: & \beta|0\rangle_c + \alpha|1\rangle_c & \xrightarrow{X} & \alpha|0\rangle_c + \beta|1\rangle_c & \xrightarrow{I} & \alpha|0\rangle_c + \beta|1\rangle_c \\ |B_{10}\rangle: & \alpha|0\rangle_c - \beta|1\rangle_c & \xrightarrow{I} & \alpha|0\rangle_c - \beta|1\rangle_c & \xrightarrow{Z} & \alpha|0\rangle_c + \beta|1\rangle_c \\ |B_{11}\rangle: & -\beta|0\rangle_c + \alpha|1\rangle_c & \xrightarrow{X} & \alpha|0\rangle_c - \beta|1\rangle_c & \xrightarrow{Z} & \alpha|0\rangle_c + \beta|1\rangle_c \end{cases}$$

Finally, qubit C is in the state $|\psi\rangle$, the same arbitrary state that A was in before the teleportation.

Notice that nothing physically "teleported" from one place to another, so "quantum teleportation" is a terrible name. Instead, teleportation is a way of using a previously established entangled pair of qubits to send another qubit without access to a quantum channel.

Just to underscore how bad the term "teleportation" is, consider its cousin technique: superdense coding.

Superdense Coding

Like quantum teleportation, Alice and Bob start with a maximally entangled Bell state between them. In teleportation, Alice sends two bits so that Bob can perform some operation on his qubit so that it matches one of Alice's.

Superdense coding is the opposite, Alice performs one of four operations on her half of the entangled pair and then sends that qubit to Bob over a quantum channel. Bob then measures the two entangled qubits in his possession in the Bell basis and attains, deterministically, one of four results. So, Alice has managed to send two bits using one qubit.

This relationship between bits, qubits, and entangled "ebits", is summarized as

$$\underbrace{1ebit + 2bits = 1qubit}_{\text{Teleportation}} \qquad \underbrace{1ebit + 1qubit = 2bits}_{\text{Superdense Coding}}$$

Assume that Alice and Bob initially share the state $|\Psi_+\rangle = \frac{|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b}{\sqrt{2}}$. If ALice wants to send the bits $j, k \in \{0, 1\}$, then she performs $X^k Z^j$ on her qubit (which is $X_a^k Z_a^j \otimes I_b$ on

the state overall) and sends it to Bob. With both qubits in hand, Bob measures them in the Bell basis and sees the state $|B_{jk}\rangle$, thus revealing the two bits.

$$\left\{\begin{array}{lccccccc} j,k & & X^k & & Z^j & & & |B_{jk}\rangle \\ j=0,k=0: & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{I_a\otimes I_b} & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{I_a\otimes I_b} & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & = & |B_{00}\rangle \\ j=0,k=1: & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{X_a\otimes I_b} & \frac{|1\rangle_a|0\rangle_b+|0\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{I_a\otimes I_b} & \frac{|1\rangle_a|0\rangle_b+|0\rangle_a|1\rangle_b}{\sqrt{2}} & = & |B_{01}\rangle \\ j=1,k=0: & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{I_a\otimes I_b} & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{Z_a\otimes I_b} & \frac{|0\rangle_a|0\rangle_b-|1\rangle_a|1\rangle_b}{\sqrt{2}} & = & |B_{10}\rangle \\ j=1,k=1: & \frac{|0\rangle_a|0\rangle_b+|1\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{X_a\otimes I_b} & \frac{|1\rangle_a|0\rangle_b+|0\rangle_a|1\rangle_b}{\sqrt{2}} & \xrightarrow{Z_a\otimes I_b} & \frac{-|1\rangle_a|0\rangle_b+|0\rangle_a|1\rangle_b}{\sqrt{2}} & = & |B_{11}\rangle \end{array}\right.$$

Quantum Key Distribution (BB84)

"Quantum cryptography" is a bit of a misnomer; the more accurate term is "quantum key distribution". In the language of cyber security, QKD is a means of generating a "shared random secret" that is robust against "man in the middle attacks". In other words, QKD allows two parties to create and share a random number while being assured that anyone listening in will be detected. Once Alice and Bob share a secret random number they can use it in a lot of ways. The most brute force use is to create a "one time pad", the only perfect (classical) security. A good message to send using that one time pad is a regular encryption key, so that Alice and Bob can continue to communicate securely over (cheap) classical communication channels. The idea here is that breaking an encryption key is hard, but breaking an unknown encryption key is a heck of a lot harder.

In the BB84 protocol, Alice and Bob use one of these two bases for every bit.

$$+ \equiv \{|\uparrow\rangle, |\rightarrow\rangle\} = \{|0\rangle, |1\rangle\} \qquad\qquad \times \equiv \{|\nearrow\rangle, |\nwarrow\rangle\} = \{|+\rangle, |-\rangle\}$$

Notice that since $|\langle 0|+\rangle|^2 = |\langle 0|-\rangle|^2 = |\langle 1|+\rangle|^2 = |\langle 1|-\rangle|^2 = \frac{1}{2}$, if a photon is prepared in one basis but measured in the other, the result will be completely random.

- Step 1) Alice produces two random N bit strings, $\{A_k\}$ and $\{a_k\}$, and Bob produces one random N bit string, $\{b_k\}$.
- Step 2) Alice uses a_k to chose the basis, $+$ or $\times$, and A_k to choose the state to send

to Bob. $\begin{cases} a_k = 0, A_k = 0 & |\psi_k\rangle = |0\rangle \\ a_k = 0, A_k = 1 & |\psi_k\rangle = |1\rangle \\ a_k = 1, A_k = 0 & |\psi_k\rangle = |+\rangle \\ a_k = 1, A_k = 1 & |\psi_k\rangle = |-\rangle \end{cases}$

- Step 3) Bob uses b_k to determine which basis to use when measuring $|\psi_k\rangle$.

  $b_k = 0 \rightarrow +$ and $b_k = 1 \rightarrow \times$. His measurements produce a new string, $\{B_k\}$.

- Step 4) Alice and Bob publicly announce $\{a_k\}$ and $\{b_k\}$ over classical channels. Together they create $\{M_k\}$ by keeping those bits in $\{A_k\}$ and $\{B_k\}$ where $a_k = b_k$ and throwing out the rest. When the bases don't match A_k and B_k are uncorrelated, so there's no sense keeping those bits.

- Step 5) Alice publicly announces a random subset of the $\{A_k\}$ she kept after step 4 and Bob compares them the same subset of $\{B_k\}$. If they are equal, then they remaining bits can be trusted and $\{M_k\}$ is their shared random number. If they correspond only 75% of the time, then there was an eavesdropper, Eve, intercepting the qubits between Alice and Bob.

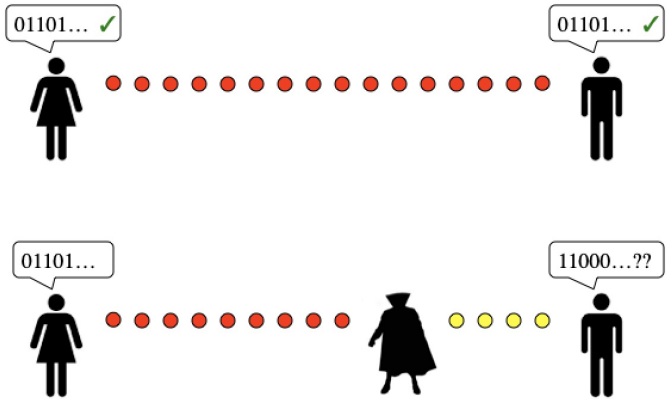

Figure 3: Because Eve can't determine which basis a photon was prepared in, she's forced to guess. Half the time she guesses right and her malfeasance goes undetected. Half the time she guesses wrong and Bob gets a random result. Eve corrupts the signal by measuring it, producing a 25% error rate which is very easy to detect over long bit strings.

If everything goes well, a typical scheme might produce something like this:

a_k	=	×	×	×	+	×	+	×	×	+	+	+	+	+	×	+	×
A_k	=	0	1	1	1	1	0	1	1	0	0	1	0	1	0	0	1
b_k	=	+	×	×	+	×	+	+	+	+	+	×	×	×	×	×	+
B_k	=	1	1	1	1	1	0	1	0	0	0	1	1	0	0	1	0
M_k	=		1	1	1	1	0			0	0				0		

When $a_k = b_k$ the photon is measured accurately and $A_k = B_k$, so the kth bit is included in Alice and Bob's shared bit string $\{M_k\}$.[6]

The central idea behind this scheme is that random bits in either basis have the same density matrix in both. For example, if Alice is sending $|0\rangle$ and $|1\rangle$ with equal probability, then in the + basis

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$$

On the other hand, if Alice is sending $|+\rangle$ and $|-\rangle$ with equal probability, then (again) in the + basis

$$\begin{aligned}
\rho &= \tfrac{1}{2}|+\rangle\langle +| + \tfrac{1}{2}|-\rangle\langle -| \\
&= \tfrac{1}{2}\left(\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\tfrac{\langle 0|+\langle 1|}{\sqrt{2}}\right) + \tfrac{1}{2}\left(\tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\tfrac{\langle 0|-\langle 1|}{\sqrt{2}}\right) \\
&= \tfrac{1}{4}|0\rangle\langle 0| + \tfrac{1}{4}|0\rangle\langle 1| + \tfrac{1}{4}|1\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1| + \tfrac{1}{4}|0\rangle\langle 0| - \tfrac{1}{4}|0\rangle\langle 1| - \tfrac{1}{4}|1\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1| \\
&= \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|
\end{aligned}$$

In other words, since the density matrices are identical, Eve (the eavesdropper) has no way of determining which basis was used or if the result they got was legitimate or random. A measurement always results is a state from the measurement basis[7], so as long as Eve successfully does a measurement, their intercepted particle is now in their measurement basis either in the correct state, if Eve guessed right, or a random state, if Eve guessed wrong.

$$|0\rangle \xrightarrow{e_k=+} |0\rangle \qquad\qquad |0\rangle \xrightarrow{e_k=\times} \begin{cases} |+\rangle, & p = \frac{1}{2} \\ |-\rangle, & p = \frac{1}{2} \end{cases}$$

Her best bet to avoid detection is to forward the state that she has to Bob. That way she'll be forwarding the correct state 50% of the time, and when she's wrong Bob's measurement will *accidentally* be correct half the time. So when Alice and Bob compare their bit streams in step 5, they'll correspond 50% + 25% = 75% of the time.

[6] It may look like $\{M_k\}$ should include more bits, since some instances when $A_k = B_k$ are not included. However, those equalities are accidental and therefore carry no information. If you guess the flip of a coin, that does not mean your guess is worth anything.

[7] This idea is so important, it's postulate 3 of only 4 (at the end of lecture 3).

If Eve is present between Alice and Bob, using $\{e_k\}$ to determine which basis to measure in, getting the results $\{E_k\}$, and sending $\begin{cases} e_k = 0, E_k = 0 & |\psi_k\rangle = |0\rangle \\ e_k = 0, E_k = 1 & |\psi_k\rangle = |1\rangle \\ e_k = 1, E_k = 0 & |\psi_k\rangle = |+\rangle \\ e_k = 1, E_k = 1 & |\psi_k\rangle = |-\rangle \end{cases}$ to Bob, then a typical run of the BB84 protocol might look like this:

a_k	=	×	×	×	+	×	+	×	×	+	+	+	+	+	×	+	×
A_k	=	0	1	1	1	1	0	1	1	0	0	1	0	1	0	0	1
e_k	=	+	×	+	×	+	+	+	×	×	×	+	+	+	+	×	+
E_k	=	1	1	1	1	1	0	0	1	1	0	1	0	1	1	0	0
b_k	=	+	×	×	+	×	+	+	+	+	+	×	×	×	×	×	+
B_k	=	1	1	1	1	1	0	0	0	**1**	0	1	1	0	**1**	0	0
M_k	=		1	1	1	1	0			!!	0				!!		

When Alice, Eve, and Bob all pick the same basis the signal sails through. If Alice and Bob choose different bases, then Eve's influence goes undetected (Alice and Bob were expecting a random result). But if Alice and Bob pick the same basis and Eve picks the other, then Bob receives noise; right half the time and wrong the other half. When Alice and Bob compare their strings, Eve is caught in the act.

The beauty of BB84 is that it can't be circumvented by Eve simply being more careful. If she successfully extracts information, then she must affect the qubits.

Exercises

#1) Another way to teleport.

Use the same circuit for teleportation used in the lecture, but change the Pauli matrices so that you can teleport using $|\Psi_-\rangle$ instead of $|\Phi_+\rangle$.

#2) Another way to code.

If Alice and Bob share the state $|\Psi_-\rangle$ and Alice would like to send Bob the bits $j = 1, k = 1$ using superdense coding. What operations should she apply to her half of the entangled pair so that when Bob receives it, the state of the entangled particles will be $|B_{11}\rangle$?

#3) Teleporting without talking.

The last state in the teleportation example, just before measuring qubits A and B, is

$$\frac{1}{2}|B_{00}\rangle_{ab}\left[\alpha|0\rangle_c + \beta|1\rangle_c\right] + \frac{1}{2}|B_{01}\rangle_{ab}\left[\beta|0\rangle_c + \alpha|1\rangle_c\right] + \frac{1}{2}|B_{10}\rangle_{ab}\left[\alpha|0\rangle_c - \beta|1\rangle_c\right] + \frac{1}{2}|B_{11}\rangle_{ab}\left[-\beta|0\rangle_c + \alpha|1\rangle_c\right]$$

It would seem that the state of qubit C is already different for different results of A and B. But can we detect the difference? Does Alice really need to send the results of the measurement to Bob? In this problem, we'll assume that Alice never sends the results of her measurements to Bob and that Bob never performs any operations to C.

a) Find the reduced density matrix of qubit C, ρ_c, before Alice makes her measurement.

b) Assume that Alice has already made her measurement and each result in the Bell basis is equally probable. Given that fact, first write down the ensemble of states for qubit C, then find the reduced density matrix of qubit C, ρ_c.

c) What effect does Alice's measurement of A and B have on Bob's qubit C?

#4) Loose lips.

Alice didn't invest in a good random number generator, so in the BB84 protocol she uses the binary expansion of π for $\{a_k\}$. Eve overheard Alice mention this, so she's ready for it.

Normally the error rate that Eve produces is 25%. What is the error rate now that Eve knows $\{a_k\}$ in advance?