QIC710/CS667/CO681/PH767/AM871 Introduction to Quantum Information Processing (F12)

**Assignment 5**
**Due date: November 29, 2012**

1. **The density matrix is in the eye of the beholder.** Consider the following scenario. Alice first flips a biased coin that has outcome 0 with probability $\cos^2(\pi/8)$ and 1 with probability $\sin^2(\pi/8)$. If the coin value is 0 she creates the state $|0\rangle$ and if the coin value is 1 she creates the state $|1\rangle$. Then Alice sends the state that she created to Bob (she does not send the coin value).

   (a) From Alice's perspective (who *knows* the coin value), the density matrix of the state she created will be either $|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ or $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. What is the density matrix of the state from Bob's perspective (who does *not* know the coin value)? Give the four matrix entries of this denisty matrix.

   (b) Suppose that, upon recieving the state from Alice, Bob measures it in the computational basis. The measurement process yields a classical bit and an output state ("collapsed" to $|0\rangle$ or $|1\rangle$). Will Bob's density matrix for the state (with Bob knowing the classical measurement outcome) be the same as Alice's?

   Suppose that we modify the above scenario to one where Alice flips a *fair* coin (where outcomes 0 and 1 each occur with probability 1/2) and if the coin value is 0 she creates the state $|\psi_0\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$ and if the coin value is 1 she creates the state $|\psi_1\rangle = \cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle$. Alice sends the state (but not the coin value) to Bob.

   (c) From Alice's perspective (who *knows* the coin value), the density matrix of the state she created will be either $|\psi_0\rangle\langle\psi_0|$ or $|\psi_1\rangle\langle\psi_1|$. What is the density matrix of the state from Bob's perspective (who does *not* know the coin value)? Give the four matrix entries of this denisty matrix.

   (d) Suppose that, upon recieving the state from Alice, Bob measures it in the computational basis, yielding a classical bit and an output state ("collapsed" to $|0\rangle$ or $|1\rangle$). Bob knows the classical bit outcome from his measurement, but does not reveal this to Alice. Will Bob's density matrix for the output state be the same as Alice's?

2. **Is the transpose a valid quantum operation?** Here we consider an operation on qubits that we denote by $\Lambda$, defined as $\Lambda(\rho) = \rho^T$ for each density matrix $\rho$ (where $\rho^T$ is the transpose of $T$).

   (a) Give an example of a one-qubit pure state $|\psi\rangle$ such that $\Lambda(|\psi\rangle\langle\psi|)$ is a pure state orthogonal to $|\psi\rangle$.

   (b) Prove that there is no unitary operation $U$ such that $\Lambda(\rho) = U\rho U^\dagger$ for all $\rho$.

   (c) **Optional for bonus credit.** Part (b) does not rule out the possibility that there is a *general quantum operation* (that is, a mapping of the form $\rho \mapsto \sum_{k=1}^m A_k \rho A_k^\dagger$, where $\sum_{k=1}^m A_k^\dagger A_k = I$) that corresponds to $\Lambda$. Show that there is no such operation.

3. **Trace distance between pure states.**
   (a) Calculate an expression for the trace distance between $|0\rangle$ and $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ as a function of $\theta$.
   (b) Calculate an expression for the Euclidean distance between the two points in the Bloch sphere that correspond to the pure states $|0\rangle$ and $\cos(\theta)|0\rangle + \sin(\theta)|1\rangle$.

4. **Secret key encryption.** Recall the classical *one-time pad* encryption scheme restricted to a single bit. The scenario is that Alice wants to send a bit of information to Bob over a channel that is possibly being monitored by Eve (an eavesdropper). We assume that Alice and Bob share a secret key, which was set up in advance. The secret key is a randomly chosen (uniformly distributed) $k \in \{0, 1\}$, which is known by Alice and Bob, but—importantly—not by Eve. If Alice wants to send a bit $m$ to Bob then Alice computes $c = m \oplus k$ and sends $c$ over the channel. When Bob receives $c$, he computes $m' = c \oplus k$. It is easy to show that $m' = m$ and Eve acquires no information about $m$ from looking at $c$. We now consider a similar scenario, but where Alice wants to send a qubit $|\psi\rangle$ to Bob over a quantum channel that is possibly being monitored by Eve. How can this be accomplished so that if Eve performs a measurement on the data that goes through the channel, she cannot acquire any information about what $|\psi\rangle$ was?
   (a) If Alice and Bob share a classical secret key bit $k \in \{0, 1\}$, then one approach would be for Alice to send $X^k|\psi\rangle$ to Bob. This seems analogous to the classical protocol: Alice either flips or doesn't flip the (qu)bit according to a random key bit. Show that this is highly insecure by giving two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$ whose encryptions Eve can perfectly distinguish between.
   (b) Suppose that Alice and Bob have two (independently generated) key bits $k_1, k_2$, and Alice encrypts $|\psi\rangle$ $Z^{k_1}X^{k_2}|\psi\rangle$. (Note that Bob can decrypt this since he has $k_1$ and $k_2$.) Show that this is perfectly secure in the sense that, for any two quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$, Eve cannot distinguish *at all* between their encryptions.

5. **A nonlocal game.** Consider the game where Alice and Bob are physically separated and their goal is to produce outputs that satisfy the winning conditions specified below. Alice and Bob receive $s, t \in \{0, 1, 2\}$ as input ($s$ to Alice and $t$ to Bob), at which point they are forbidden from communicating with each other (so Alice has no idea what $t$ is and Bob has no idea what $s$ is). They each output a bit, $a$ for Alice and $b$ for Bob. The winning conditions are:
   - $a = b$ in the cases where $s = t$.
   - $a \neq b$ in the cases where $s \neq t$.

   (a) Show that any classical strategy (that uses no quantum information) of Alice and Bob that always succeeds in the $s = t$ cases can succeed with probability at most $2/3$ in the $s \neq t$ cases.
   (b) Give a quantum strategy (that is, one where Alice and Bob can create an entangled state before the game starts and then base their outcomes on their measurements of their parts of this state) that always succeeds in the $s = t$ cases and succeeds with probability $3/4$ in the $s \neq t$ cases. (Hint: try the entangled state $\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$ and have Alice and Bob perform rotations depending on $s$ and $t$ respectively.)