Assignment 3 - due April 13th

- This assignment corresponds to the material in Lectures 4 to 7.
- Lecture 4 was about composing systems. We discussed reduced states, partial trace, and two applications: superdense coding and quantum teleportation. It corresponding to sections 2.3 and 2.4 of Nielsen's, or 3.5 and 3.6 of Wilde's.
- Lecture 5 is about Schmidt's decomposition and purification. It corresponds roughly to Section 2.5 of Nielsen's or 3.8 of Wilde's. It also introduced the problem of distinguishing states, corresponding basically to Section 2.2.4 of Nielsen's.
- Lecture 6 introduces POVMs. You will find it in 2.2.6 of Nielsen's, or more generally Chapter 4 of Barnett's.
- Lecture 7 is about fidelity and quantum channels. Chapter 9 of Nielsen's, but more nicely the end of Chapter 2 and beginning of Chapter 3 of Preskill's.

Exercise 1. @

Consider the superdense coding protocol, in which Alice sends Bob a qubit with the intent of transmitting two qubits of information. Suppose a third party Eve intercepts Alice's qubit. Can she infer anything about which of the four possible bit strings Alice is trying to send? If so, how? If not, why not?

Exercise 2. @

Show an example of a state in a three party system for which a Schmidt decomposition is not available.

Exercise 3. @

Let ρ be a mixed state, which can be realized in the following two ways:

$$\rho = \sum_i p_i |a_i\rangle\langle a_i| = \sum_i q_i |b_i\rangle\langle b_i|.$$

Find one purification for ρ which allows for either way to be obtained depending only on the observable that is used. Derive an expression for each observable.

Exercise 4. @

Assume $\{M_1, ..., M_m\}$ is a POVM, and ρ is a density matrix. Let $\{|i\rangle\}_{i=1}^m$ be a basis of an m dimensional system. Prove that

$$\rho' = \sum_{i=1}^m M_i \rho M_i^* \otimes |i\rangle\langle i|.$$

is a density matrix.

Exercise 5.

Let $|a\rangle$ and $|b\rangle$ be states, and $|a^\perp\rangle$ and $|b^\perp\rangle$ be perpendicular states to each respectively. Let

$$M_a = \frac{1}{1 + |\langle a|b\rangle|} |a^\perp\rangle\langle a^\perp| \quad \text{and} \quad M_b = \frac{1}{1 + |\langle a|b\rangle|} |b^\perp\rangle\langle b^\perp|.$$

Show that $I - M_a - M_b$ is positive semidefinite.

Exercise 6.
Alice and Bob are each given one of the qubits of some 2-qubit state. Working as a team, they are required to distinguish between State I and State II with only local projective measurements. That means, they can each measure their own qubit according to some observable. After their measurements, they can send only classical bits to each other.

In each case below, either give a perfect distinguishing procedure or explain why there is no perfect distinguishing procedure.

(a)
$$\text{State 1: } \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{and} \quad \text{State 2: } \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

(b)
$$\text{State 1: } \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{and} \quad \text{State 2: } \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

(c)
$$\text{State 1: } \frac{1}{\sqrt{2}}(|00\rangle + \mathrm{i}|11\rangle) \quad \text{and} \quad \text{State 2: } \frac{1}{\sqrt{2}}(|00\rangle - \mathrm{i}|11\rangle)$$

Exercise 7.

Recall that in the teleportation protocol, Alice and Bob have a joint state of the form

$$(\alpha|0\rangle_A + \beta|1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}),$$

where subscripts are indicating who possesses each qubit. At the end of the protocol, Bob's qubit is at state $(\alpha|0\rangle_B + \beta|1\rangle_B)$.

Suppose that Alice's qubit which is going to be teleported is actually entangled with Charlie's, in state

$$\frac{1}{\sqrt{2}}(|00\rangle_{CA} + |11\rangle_{CA}).$$

Assume now Alice and Bob execute the teleportation protocol regardless. At the end, will the joint state of Charlie's and Bob's qubits be

$$\frac{1}{\sqrt{2}}(|00\rangle_{CB} + |11\rangle_{CB})?$$

Justify your answer.

Exercise 8.

Alice wishes to commit a bit to Bob, and later he is supposed to unveil the value of the bit. This procedure is called binding if Alice is unable to change the value of her bit after

commitment, and is called concealing if Bob is unable to check the value of the bit until the unveiling moment. The protocol is called secure if it is both binding and concealing.

Classically, one way to attempt this is for Alice to send her bit in a safe, and only at the unveiling phase she reveals the safe's secret. The process is concealing so as long as Bob is not a good safe cracker.

Quantumly, here is a proposition. Alice prepares one of two distinguishable density operators ρ_0 and ρ_1 in a bipartite system AB, sends system B to Bob, and keeps A to herself. Later, to unveil, she sends A to Bob, and he performs a measurement to determine whether it is ρ_0 or ρ_1.

Show that if a quantum bit commitment protocol is concealing, then it is not binding. Thus quantum bit commitment is insecure.

(you may assume that both states to be used are pure, but it would be nice to argue why this is possible as well)