Ph 219a/CS 219a

Exercises
Due: Wednesday 26 October 2005

1.1 Alice does Bob a favor

Alice, in Anaheim, and Bob, in Boston, share a bipartite pure state $|\Psi\rangle$, which can be expressed in the Schmidt form

$$|\Psi\rangle = \sum_i \sqrt{p_i}\ |\alpha_i\rangle \otimes |\beta_i\rangle\ , \tag{1}$$

where $\{|\alpha_i\rangle\}$ is an orthonormal basis for Alice's system A, $\{|\beta_i\rangle\}$ is an orthonormal basis for Bob's system B, and the $\{p_i\}$ are nonnegative real numbers summing to 1. Bob is supposed to perform a complete orthogonal local measurement on B, characterized by the set of projectors $\{E_a^B\}$ — if the measurement outcome is a, then Bob's measurement prepares the state

$$|\Psi\rangle \mapsto |\Psi_a\rangle = \frac{\left(I \otimes E_a^B\right)|\Psi\rangle}{\langle\Psi|\left(I \otimes E_a^B\right)|\Psi\rangle^{1/2}}\ . \tag{2}$$

$|\Psi_a\rangle$ can also be expressed in the Schmidt form if we choose appropriate orthonormal bases for A and B that depend on the measurement outcome. The new Schmidt basis elements can be written as

$$|\alpha'_{a,i}\rangle = U_a^A|\alpha_i\rangle\ , \quad |\beta'_{a,i}\rangle = U_a^B|\beta_i\rangle\ , \tag{3}$$

where U_a^A, U_a^B are unitary.

Unfortunately, Bob's measurement apparatus is broken, though he still has the ability to perform local unitary transformations on B. Show that Alice can help Bob out by performing a measurement that is "locally equivalent" to Bob's. That is, there are orthogonal projectors $\{E_a^A\}$ and unitary V_a^A, V_a^B such that

$$|\Psi_a\rangle = V_a^A \otimes V_a^B \left(\frac{\left(E_a^A \otimes I\right)|\Psi\rangle}{\langle\Psi|\left(E_a^A \otimes I\right)|\Psi\rangle^{1/2}}\right)\ , \tag{4}$$

and furthermore, both Alice's measurement and Bob's yield outcome a with the same probability. This means that instead of Bob doing the measurement, the same effect can be achieved if Alice measures instead, tells Bob the outcome, and both Alice and Bob perform the appropriate unitary transformations. Construct E_a^A (this is most conveniently done by expressing both E_a^A and E_a^B in the Schmidt bases for $|\Psi\rangle$) and express V_a^A and V_a^B in terms of U_a^A and U_a^B.

Remark: This result shows that for any protocol involving local operations and "two-way" classical communication (2-LOCC) that transforms an initial bipartite pure state to a final bipartite pure state, the same transformation can be achieved by a "one-way" (1-LOCC) protocol in which all classical communication is from Alice to Bob (the *Lo-Popescu Theorem*). In a two-way LOCC protocol, Alice and Bob take turns manipulating the state for some finite (but arbitrarily large) number of rounds. In each round, one party or the other performs a measurement on her/his local system and broadcasts the outcome to the other party. Either party might use a local "ancilla" system in performing the measurement, but we may include all ancillas used during the protocol in the bipartite pure state $|\Psi\rangle$. Though a party might discard information about the measurement outcome, or fail to broadcast the information to the other party, we are entitled to imagine that the complete information about the outcomes is known to both parties at each step (incomplete information is just equivalent to the special case in which the parties choose not to use all the information). Thus the state is pure after each step.

The solution to the exercise shows that a round of a 2-LOCC protocol in which Bob measures can be simulated by an operation performed by Alice and a local unitary applied by Bob. Thus, we can allow Alice to perform all the measurements herself. When she is through she sends all the outcomes to Bob, and he can apply the necessary product of unitary transformations to complete the protocol.

1.2 What probability distributions are consistent with a mixed state?

A density operator ρ, expressed in the orthonormal basis $\{|\alpha_i\rangle\}$ that diagonalizes it, is

$$\rho = \sum_i p_i |\alpha_i\rangle\langle\alpha_i| \ . \tag{5}$$

We would like to realize this density operator as an ensemble of pure states $\{|\varphi_\mu\rangle\}$, where $|\varphi_\mu\rangle$ is prepared with a specified probability q_μ. This preparation is possible if the $|\varphi_\mu\rangle$'s can be chosen so that

$$\rho = \sum_\mu q_\mu |\varphi_\mu\rangle\langle\varphi_\mu| \ . \tag{6}$$

We say that a probability vector q (a vector whose components are nonnegative real numbers that sum to 1) is *majorized* by a probability vector p (denoted $q \prec p$), if there exists a *doubly stochastic* matrix D such that

$$q_\mu = \sum_i D_{\mu i}\ p_i \ . \tag{7}$$

A matrix is doubly stochastic if its entries are nonnegative real numbers such that $\sum_\mu D_{\mu i} = \sum_i D_{\mu i} = 1$. That the columns sum to one assures that D maps probability vectors to probability vectors (*i.e.*, is *stochastic*). That the rows sum to one assures that D maps the uniform distribution to itself. Applied repeatedly, D takes any input distribution closer and closer to the uniform distribution (unless D is a permutation, with one nonzero entry in each row and column). Thus we can view majorization as a partial order on probability vectors such that $q \prec p$ means that q is more nearly uniform than p (or equally close to uniform, in the case where D is a permutation).

Show that normalized pure states $\{|\varphi_\mu\rangle\}$ exist such that eq. (6) is satisfied if and only if $q \prec p$, where p is the vector of eigenvalues of ρ.

Hint: Use the *Hughston-Jozsa-Wootters Theorem.* You may also use (but need not prove) *Horn's Lemma*: if $q \prec p$, then there exists a unitary (in fact, orthogonal) matrix $U_{\mu i}$ such that $q = Dp$ and $D_{\mu i} = |U_{\mu i}|^2$.

1.3 What transformations are possible for bipartite pure states?

Alice and Bob share a bipartite pure state $|\Psi\rangle$. Using a 2-LOCC protocol, they wish to transform it to another bipartite pure state $|\Phi\rangle$. Furthermore, the protocol must be *deterministic* — the state $|\Phi\rangle$ is obtained with probability one irrespective of the outcomes of the measurements that Alice and Bob perform.

Suppose that these initial and final states have Schmidt decompositions

$$|\Psi\rangle = \sum_i \sqrt{p_\Psi}\ |\alpha_i\rangle \otimes |\beta_i\rangle\ , \quad |\Phi\rangle = \sum_i \sqrt{p_\Phi}\ |\alpha_i'\rangle \otimes |\beta_i'\rangle\ . \qquad (8)$$

Show that if the deterministic transformation $|\Psi\rangle \mapsto |\Phi\rangle$ is possible, then $p_\Psi \prec p_\Phi$.

Hints: Use the Lo-Popescu Theorem from Exercise 1.1 to reduce the 2-LOCC to an equivalent 1-LOCC. Recall that a generalized measurement is defined by a set of operators $\{M_\mu\}$ such that $\sum_\mu M_\mu^\dagger M_\mu = I$, and that the action of the measurement on a pure state $|\psi\rangle$ if outcome μ occurs is

$$|\psi\rangle \mapsto \frac{M_\mu|\psi\rangle}{\sqrt{\langle\psi|M_\mu^\dagger M_\mu|\psi\rangle}}\ . \qquad (9)$$

You also might want to keep in mind the *polar decomposition*: a matrix A can be expressed as $\sqrt{AA^\dagger}\ U$, where U is unitary.

Remark: The converse is also true. Thus majorization provides the necessary and sufficient condition for the deterministic transformation of one bipartite pure state to another (*Nielsen's Theorem*). In this respect, majorization defines a partial order on bipartite pure states such that we may say that $|\Psi\rangle$ is no less entangled than $|\Phi\rangle$ if $p_\Psi \prec p_\Phi$.

1.4 Quantum bit commitment

The White Sox are going to play the Astros in the World Series. Alice is sure that she knows who will win. Alice doesn't like Bob, so she doesn't want to tell him who the winner will be. But after the Series is over, Alice wants to be able to convince Bob that she knew the outcome all along. What to do?

Bob suggests that Alice write down her choice (0 if the White Sox will win, 1 if the Astros will win) on a piece of paper, and lock the paper in a box. She is to give the box to Bob, but she will keep the key for herself. Then, when she is ready to reveal her choice, she will send the key to Bob, allowing him to open the box and read the paper.

Alice rejects this proposal. She doesn't trust Bob, and she knows that he is a notorious safe cracker. Who's to say whether he will be able to open the box and sneak a look, even if he doesn't have the key?

Instead, Alice proposes to certify her honesty in another way, using quantum information. To *commit* to a value $a \in \{0,1\}$ of her bit, she prepares one of two distinguishable density operators (ρ_0 or ρ_1) of the bipartite system AB, sends system B to Bob, and keeps system A for herself. Later, to *unveil* her bit, Alice sends system A to Bob, and he performs a measurement to determine whether the state of AB is ρ_0 or ρ_1. This protocol is called *quantum bit commitment*

We say that the protocol is *binding* if, after commitment, Alice is unable to change the value of her bit. We say that the protocol is *concealing* if, after commitment and before unveiling, Bob is unable to discern the value of the bit. The protocol is *secure* if it is both binding and concealing.

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

Hint: First argue that without loss of generality, we may assume that the states ρ_0 and ρ_1 are both pure. Then apply the Hughston-Jozsa-Wootters Theorem.

Remark: Note that the conclusion that quantum bit commitment is insecure still applies even if the shared bipartite state (ρ_0 or ρ_1) is prepared during many rounds of quantum communication between Alice and Bob, where in each round one party performs a quantum operation on his/her local system and on a shared message system, and then sends the message system to the other party.