Quantum Computing and Information - Problem Set 4 **Due Wed, Mar 9, 2011**

Exercise 1. **Fidelity and trace distance**

a) Give an exact relation between $F(\alpha,\beta)$ and $T := \frac{1}{2}\|\alpha-\beta\|_1$ for pure states $\alpha = |\alpha\rangle\langle\alpha|$ and $\beta = |\beta\rangle\langle\beta|$.

b) Use this to prove that $F(\rho,\sigma)^2 \leq 1 - \frac{1}{4}\|\rho-\sigma\|_1$ for general density matrices ρ,σ.

Exercise 2. **Optimality of super-dense coding and teleportation**

a) Suppose that Alice would like to transmit an n-bit message x to Bob, but has access only to m uses of a noiseless bit channel, for $m \leq n$. Assume that x is drawn uniformly at random. Prove that for any encoding/decoding strategy, Bob's probability of guessing x is $\leq 2^{m-n}$.

b) Show that this bound still holds if Alice and Bob share an arbitrary entangled state $|\psi\rangle \in \mathbb{C}^{d\times d}$.

c) Can the communication cost of teleportation be improved, possibly at the cost of using more entanglement? Specifically, is it possible to exactly teleport n qubits using some large amount of entanglement, but using $< 2n$ bits of communication?

d) Similarly, can the communication cost of super-dense coding be improved, again possibly at the cost of using more entanglement? Specifically, is it possible to transmit $2n$ cbits using some large amount of entanglement, but $< n$ qubits of communication?

e) *Optional:* Prove that n qubits cannot be teleported using fewer than n copies of $|\Phi_2\rangle$ and an unlimited amount of classical communication. *Hint: show that local operations and classical communication has zero probability of increasing the number of nonzero Schmidt coefficients of an entangled state.*

Exercise 3. **Partial Transpose and Data Hiding**

a) Define the transpose map $T : M_d \to M_d$ by $T(X) = X^T$. Show that T is positive but not completely positive.

b) Show that $(\mathrm{id} \otimes T)(\rho^{AB}) \geq 0$ for any $\rho \in \mathrm{SEP}(d_A, d_B)$, where SEP is the set of separable states defined in problem set 3. The operator $\mathrm{id} \otimes T$ is called the *partial transpose*.

c) Define the class of LOCC (Local Operations + Classical Communication) operations on $\mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ to consist of all finite-length sequences of measurements by Alice on her system (followed by sending the measurement result to Bob) and measurement by Bob of his system (followed by sending the measurement result to Alice). Note that measurements can be chosen based on the previous communication record. Prove that every quantum operation $\mathcal{N}$ in LOCC has the form

$$\mathcal{N}(\rho) = \sum_j (X_j^A \otimes Y_j^B)\rho^{AB}(X_j^A \otimes Y_j^B)^\dagger.$$

d) Suppose that $\{M, I-M\}$ is a 2-outcome measurement that is implemented by LOCC. Prove that

$$0 \leq (\mathrm{id} \otimes T)(M) \leq I \tag{1}$$

e) Let $F = \sum_{i,j=1}^d |i,j\rangle\langle j,i|$ denote the unitary operator that swaps the states of two quantum system. Compute $(\mathrm{id} \otimes T)(F)$ and write down its eigenvalues.

f) Since $F^2 = I$, it follows that the eigenvalues of F are ± 1. Define the projectors $\Pi_\pm = (I \pm F)/2$ and the *data-hiding* states $\rho_\pm = \Pi_\pm / \mathrm{tr}\,\Pi_\pm$. Consider a measurement

$$M = m_+\Pi_+ + m_-\Pi_-. \tag{2}$$

Define the *bias* of M to be $\mathrm{tr}\, M(\rho_+ - \rho_-)$. Calculate the maximum bias for (i) any valid measurement M, and (ii) any M satisfying Eq. (1). What can you say about the distinguishability of $\rho_\pm$ when Alice and Bob are restricted to LOCC measurements? Is the "data-hiding" name appropriate?

g) *Optional:* Prove that the optimal bias (either with or without the requirement that Eq. (1) be satisfied) is achieved by M of the form in Eq. (2).