Quantum Computing and Information - Problem Set 3 **Due Wed, Feb 23, 2011**

Exercise 1. Prove that $\operatorname{tr}\rho^2 \leq 1$ with equality iff ρ is pure (i.e. of the form $|\psi\rangle\langle\psi|$.

Exercise 2. Prove that the extreme points of $\mathcal{D}(\mathbb{C}^d)$ are the pure states.

Exercise 3. Alice and Bob share the state

$$|\psi\rangle^{AB} = \sum_{i=1}^{d_A}\sum_{j=1}^{d_B} A_{i,j}\,|i\rangle^A \otimes |j\rangle^B .$$

Calculate Bob's reduced density matrix. Like the expression derived in class for Alice's reduced density matrix, your expression should not have any subscripts or summation signs in it.

Exercise 4. **Bit commitment** Alice and Bob have been playing a grueling game of chess and by the end of the first day, it's Alice's move and they've only reached the midgame. Alice has only two choices of move (0 or 1), but if she tells Bob then he'll be able to spend all night planning his response. On the other hand, if Alice doesn't tell him her move until morning then *she* could get an unfair advantage by thinking about her move all night.

Bob suggests that Alice could write her move on a piece of paper and give it to him in a sealed envelope. But Alice knows that Bob could easily steam the envelope open, read the paper and reseal the envelope. Instead she proposes to use quantum mechanics.

Her idea is to prepare one of two distinguishable states $|\psi_0\rangle^{AB}$ or $|\psi_1\rangle^{AB}$ and give system B to Bob at night, keeping A for herself. Thus she *commits* to her bit $a \in \{0,1\}$. Then she *reveals* a in the morning by sending system A to Bob and he performs a measurement to determine whether the state of AB is $|\psi_0\rangle$ or $|\psi_1\rangle$.

Ideally the protocol would be *concealing* if Bob could not learn any information about a after Alice commits her bit and before she reveals it (i.e. from system B alone). On the other hand, it should also be *binding*, meaning that after committing her bit, Alice is unable to change its value.

Show that both properties cannot simultaneously hold: no commitment protocol can be both concealing and binding.

Exercise 5. **Separable states**

a) Let S be a set in $\mathbb{R}^d$. Prove that any $x \in \operatorname{conv}(S)$ can be written as a convex combination of $d+1$ points in S. That is, there exist $p_1,\ldots,p_{d+1} \geq 0$, $y_1,\ldots,y_{d+1} \in S$ such that $\sum_{i=1}^{d+1} p_i = 1$ and

$$x = \sum_{i=1}^{d+1} p_i y_i.$$

Hint: Suppose that $x = \sum_{i=1}^m p_i y_i$ for some $m > d+1$. Then prove the existence of a vector $q \in \mathbb{R}^m$ satisfying $\sum_{i=1}^m q_i = 0$ and $\sum_{i=1}^m q_i y_i = 0$ and consider replacing p with $p - tq$ for some cleverly chosen $t \in \mathbb{R}$.

b) Let $\mathrm{SEP}(d_A, d_B) \subset \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ denote the set of *separable states*, defined to be the set of states ρ^{AB} that can be written in the form

$$\rho^{AB} = \sum_i p_i \sigma_i^A \otimes \omega_i^B,$$

where $\sum_i p_i = 1$, each $p_i \geq 0$, $\sigma_i \in \mathcal{D}(\mathbb{C}^{d_A})$ and $\omega_i \in \mathcal{D}(\mathbb{C}^{d_B})$. We call states of the form $\sigma \otimes \omega$ *product states* and can equivalently say that separable states are the convex hull of product states. States that are not separable are said to be *entangled*.

Prove that any $\rho^{AB} \in \mathrm{SEP}(d_A, d_B)$ can be written as a convex combination of $d_A^2 d_B^2$ product pure states.

Exercise 6. **Trace distance** Suppose that you are given one of two possible d-dimensional states σ_1 or σ_2, with probabilities p_1 and $p_2 = 1 - p_1$ respectively. Your task is to perform a two-outcome measurement and then try to guess which state you had been given, minimising the probability of error.
If the measurement elements are nonnegative Hermitian matrices M_1 and $M_2 = I - M_1$ then the probability of guessing wrong is

$$P_{err} = p_1 \operatorname{tr}(\sigma_1 M_2) + p_2 \operatorname{tr}(\sigma_2 M_1).$$

a) Show that

$$P_{\text{err}} = p_1 - \sum_{i=1}^{d} \lambda_i \langle i| M_1 |i\rangle ,$$

where $|i\rangle$ denotes the orthonormal basis of eigenstates of the Hermitian operator $p_2\sigma_2 - p_1\sigma_1$ and the λ_i are the corresponding eigenvalues.

b) Find the nonnegative operator M_1 that minimizes P_{err}. Show that the resulting error probability is $P_{err,opt} = p_1 - \sum_{i:\lambda_i<0} |\lambda_i|$. *Hint: Express M_1 in the $|i\rangle$ basis.*

c) For a Hermitian matrix A, define $|A|$, the absolute value of A, as follows: write $A = UDU^\dagger$ for

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots 0 & \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ & & & & \\ 0 & 0 & \ddots & 0 & 0 \\ & & & & \\ 0 & \dots & & & \lambda_d \end{pmatrix}$$

and U unitary, and then

$$|A| = U \begin{pmatrix} |\lambda_1| & 0 & 0 & \cdots 0 & \\ 0 & |\lambda_2| & 0 & \cdots & 0 \\ & & & & \\ 0 & 0 & \ddots & 0 & 0 \\ & & & & \\ 0 & \dots & & & |\lambda_d| \end{pmatrix} U^\dagger.$$

Express the trace norm $\|p_2\sigma_2 - p_1\sigma_1\|_1 := \operatorname{tr}|p_2\sigma_2 - p_1\sigma_1|$ in terms of the eigenvalues λ_i. Use this, together with the fact that $\operatorname{tr}(p_2\sigma_2 - p_1\sigma_1) = \sum_i \lambda_i = p_2 - p_1$, to express $P_{err,opt}$ as a function of $\|p_2\sigma_2 - p_1\sigma_1\|_1$.

d) Evaluate $P_{err,opt}$ in the following cases:

i) $p_1 = 1$, $p_2 = 0$ and σ_1, σ_2 are arbitrary.

ii) $p_1 = p_2 = 1/2$, $\sigma_1 = |\psi_1\rangle\langle\psi_1|$, $\sigma_2 = |\psi_2\rangle\langle\psi_2|$, with $|\psi_1\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ and $|\psi_2\rangle = \sin(\theta)|0\rangle + \cos(\theta)|1\rangle$. Check that your answer makes sense when θ is 0 or $\pi/4$.

Exercise 7. **Purifications** Let ρ^A be a density matrix and $|\psi\rangle^{AB}$ an arbitrary purification of ρ.

a) Consider a decomposition $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$, where $|\varphi_i\rangle$ are not necessarily orthogonal to each other, and $\{p_i\}$ is a probability distribution. Find a measurement on B such that when applied to half of $|\psi\rangle$ outcome i occurs with probability p_i and Alice's residual state is $|\varphi_i\rangle$.

b) What if we decompose ρ into $\rho = \sum_i p_i\sigma_i$ for general density matrices σ_i? Is it still possible to find a measurement on B such that outcome i occurs with probability p_i and the residual state for Alice is σ_i?

c) Let $\mathcal{N}$ be a quantum operation. The *entanglement fidelity* measures how well it approximates the identity on ensembles with density matrix ρ, and is defined

$$F_e(\mathcal{N}, \rho) := \sqrt{\langle\psi| (\mathcal{N} \otimes \mathrm{id})(\psi) |\psi\rangle},$$

where $|\psi\rangle$ is an arbitrary purification of ρ and $\psi := |\psi\rangle\langle\psi|$. Prove that F_e does not depend on the purification chosen, and therefore that F_e is well defined.

d) Prove that $\sum_i p_i \langle\varphi_i|\mathcal{N}(\varphi_i)|\varphi_i\rangle \geq F_e$ for any ensemble satisfying $\rho = \sum_i p_i \varphi_i$.