Quantum Information Basics: Patrick Hayden

Problems

1. *Partial transposition and entanglement.*

A density operator ρ^{AB} on a bipartite system $A \otimes B$ is *separable* if it can be written as a convex combination of product states: $\rho^{AB} = \sum_i p_i \, \sigma_i^A \otimes \omega_i^B$, where $\sum_i p_i = 1$, $p_i \geq 0$ and all the σ_i^A and ω_i^B are density operators. Density operators that are not separable are said to be *entangled*. In this problem, you will study one way of distinguishing entangled states from separable states. Because of the ensemble ambiguity of the density operator, it isn't obvious how to determine whether a state is entangled; if there exists a single ensemble which is a mixture of product states then the state is separable so how can we ever be sure without checking all possible ensembles?

a) Show that the transpose map $T(X) = Y$ where $Y_{ij} = X_{ji}$ is positive but not completely positive. That is, T always takes positive semidefinite operators to positive semidefinite operators, but $I \otimes T$ does not. *Hint:* Let T act on half of a maximally entangled pair of qubits.

b) Show that $(\mathrm{id} \otimes T)(\rho_{AB})$ is positive semidefinite for any separable density operator ρ_{AB}. ($\mathrm{id} \otimes T$ is called the *partial transpose* just as $\mathrm{id} \otimes \mathrm{Tr}$ is the partial trace.)

You have therefore demonstrated that the partial transpose can be used to test for the presence of entanglement. The test isn't conclusive, though. If the partial transpose of ρ is not positive semidefinite then ρ must be entangled, but sometimes states that are entangled will nonetheless have positive semidefinite partial transposes. (The test *is* conclusive for pairs of qubits, though.)

2. *Bit commitment.*

Alice and Bob don't trust each other but would like to jointly execute a computation. One of the basic primitives from which they can build up the ability to perform complicated secure two-party computations is *bit commitment*. The idea is to mimic the functionality of a safe: Alice locks a bit in the safe and then transfers the safe to Bob. At some time in the future, Alice tells Bob the combination so that he can look inside the safe and determine the value of Alice's bit.

We will restrict our attention to protocols of the following form:

- **Commitment phase:** Alice selects a bit $b \in \{0, 1\}$. She then prepares a state $|\psi^{(b)}\rangle_{AB_1B_2}$ and sends the B_1 system to Bob.
- **Reveal phase:** Alice sends the B_2 system to Bob. He performs a POVM measurement $\{M_0, M_1\}$ on B_1B_2 and announces j as the value of the bit when M_j occurs.

An ideal bit commitment protocol has the following properties:

- **Hiding**: When Alice follows the protocol, the density operator $\psi_{B_1}^{(b)} = \mathrm{Tr}_{AB_2} |\psi^{(b)}\rangle\langle\psi^{(b)}|_{AB_1B_2}$ is independent of b. Bob therefore can't learn anything about b before the reveal phase.
- **Binding:** A dishonest Alice cannot change her mind after the commitment phase. In other words, it is impossible for Alice to change $|\psi^{(b)}\rangle$ into $|\psi^{(\neg b)}\rangle$ after the completion of the commitment phase.

a) Argue that if $|\varphi\rangle_{AB}$ and $|\psi\rangle_{AB}$ satisfy $\varphi_A = \psi_A$ then there exists a unitary transformation U acting on B such that $(I \otimes U)|\varphi\rangle_{AB} = |\psi\rangle_{AB}$. *Hint:* Schmidt decomposition.

b) Show that ideal bit commitment is impossible.

There is a highly cited paper from the nineties purporting to show that quantum mechanics makes it possible to implement secure bit commitment. It was wrong, as you've demonstrated. (The full argument is actually a bit more subtle because it must take into account fancier kinds of protocols including classical and bidirectional communication, but the spirit is the same.)

3. *Quantum Pinsker's inequality.*

The goal of this problem is to prove an inequality between the relative entropy and the trace distance. You'll then derive a widely used consequence, which is a bound on correlators in terms of mutual information.

a) The trace distance between two density operators ρ and σ can be expressed in terms of the outcome probabilities of the optimal measurement for distinguishing them, known as the Helstrom measurement. The POVM operators of the Helstrom measurement are orthogonal projectors Π_+ and Π_- onto the positive (technically, nonnegative) and negative eigenspaces of $\rho - \sigma$. Let $r_\pm = \operatorname{tr} \Pi_\pm \rho$ and $s_\pm = \operatorname{tr} \Pi_\pm \sigma$ be the outcome probability distributions for the two states. Show that $\|\rho - \sigma\|_1 = \|r - s\|_1$.

b) Show that for binary random variables r and s,

$$S(r\|s) \geq \frac{1}{2}\|r - s\|_1^2. \tag{1}$$

Hint: First express $S(r\|s)$ and $\|r - s\|_1^2$ in terms of r_+ and s_+. Then differentiate $S(r\|s) - \|r - s\|_1^2/2$ with respect to s_+.

c) Combine your previous results with monotonicity to finish the proof of the quantum Pinsker inequality:

$$S(\rho\|\sigma) \geq \frac{1}{2}\|\rho - \sigma\|_1^2. \tag{2}$$

d) Confirm that for a density operator ρ_{AB} of a composite system that $I(A;B) = S(\rho_{AB}\|\rho_A \otimes \rho_B)$.

e) Note that $\|X\|_1 = \max_{\|\mathcal{O}\|_\infty \leq 1} \operatorname{tr} X\mathcal{O}$, where $\|\mathcal{O}\|_\infty$ is the largest singular value of $\mathcal{O}$. (You can assume this: it is a special case of Hölder's inequality for the Schatten-ℓ_p spaces.) For operators $\mathcal{O}_A$ and $\mathcal{O}_B$ acting respectively only on A and B, show that

$$I(A;B)_\rho \geq \frac{1}{2}\left(\frac{\langle \mathcal{O}_A \otimes \mathcal{O}_B\rangle_\rho - \langle \mathcal{O}_A\rangle_\rho \langle \mathcal{O}_B\rangle_\rho}{\|\mathcal{O}_A\|_\infty \|\mathcal{O}_B\|_\infty}\right)^2. \tag{3}$$

4. *A useful POVM.*

Let $|\varphi\rangle$ and $|\psi\rangle$ be states in $\mathbb{C}^2$ such that $\langle\varphi|\psi\rangle = \alpha$. Choose states $|\varphi^\perp\rangle, |\psi^\perp\rangle \in \mathbb{C}^2$ such that $\langle\varphi|\varphi^\perp\rangle = \langle\psi|\psi^\perp\rangle = 0$. For $\lambda \in \mathbb{R}$, consider the triple of operators

$$E_1 = \lambda|\varphi^\perp\rangle\langle\varphi^\perp|, \quad E_2 = \lambda|\psi^\perp\rangle\langle\psi^\perp|, \quad E_3 = I - E_1 - E_2. \tag{4}$$

a) For which values of λ does $\{E_1, E_2, E_3\}$ form a POVM?

b) Consider the POVM with the largest such λ. If this POVM is applied to an unknown state which is either $|\varphi\rangle$ or $|\psi\rangle$, outcome E_1 implies the state must have been $|\psi\rangle$ while outcome E_2 implies the state must have been $|\varphi\rangle$. Explain why this does *not* provide a counterexample to the impossibility of perfectly distinguishing nonorthogonal states.

c) Suppose you are given a quantum state chosen from a set $\{|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle\}$ of linearly independent states. Construct a POVM $\{E_1, E_2, \ldots, E_{m+1}\}$ such that if outcome E_j occurs for $1 \leq j \leq m$, then you can conclude with certainty that you were given state $|\varphi_j\rangle$. Your POVM must be such that $\langle\varphi_j|E_j|\varphi_j\rangle > 0$ for $1 \leq j \leq m$.