C&O 781 Topics in Quantum Information

Quantum Information Theory, Error-correction, and Cryptography
University of Waterloo
Spring 2008

Instructors: Debbie Leung and Ashwin Nayak
Assignment 3, Jun 27, 2008
Due: Jul 11, 2008

In the following questions, $\mathcal{H}$ and $\mathcal{K}$ are finite dimensional Hilbert spaces.

Question 1. [5 marks] For any $M \in \mathrm{L}(\mathcal{H})$, prove that

$$\max_{\text{unitary } U \in \mathrm{L}(\mathcal{H})} |\mathrm{Tr}(UM)| \quad = \quad \|M\|_{\mathrm{tr}}.$$

Conclude that

$$\|A+B\|_{\mathrm{tr}} \quad \leq \quad \|A\|_{\mathrm{tr}} + \|B\|_{\mathrm{tr}}$$

for all $A, B \in \mathrm{L}(\mathcal{H})$. (Therefore, the function $\|\cdot\|_{\mathrm{tr}} : \mathrm{L}(\mathcal{H}) \to \mathbb{R}$ is a norm.)

Question 2. [5 marks] Prove that for any density matrices $\rho_0, \rho_1 \in \mathrm{L}(\mathcal{H})$,

$$\max_{\text{quantum states } \sigma \in \mathrm{L}(\mathcal{H})} \left(\mathrm{F}(\rho_0, \sigma) + \mathrm{F}(\sigma, \rho_1)\right) \quad = \quad 1 + \sqrt{\mathrm{F}(\rho_0, \rho_1)}\,.$$

Hint: first consider pure states ρ_0, ρ_1.

Question 3. [5 marks] Show that for single qubit states $\rho_0, \rho_1 \in \mathrm{L}(\mathcal{H})$,

$$1 - \mathrm{F}(\rho_0, \rho_1) \quad \leq \quad \frac{1}{2}\|\rho_0 - \rho_1\|_{\mathrm{tr}}.$$

Note that this is a stronger lower bound on trace distance in terms of fidelity than the general bound we saw in class.

Question 4. [5 marks] In the strong coin flipping protocol (with cheating probability 3/4) we saw in class, we used qutrit states $|\psi_a\rangle \in \mathbb{C}^3 \otimes \mathbb{C}^3$. Find the best protocol of the same form, using bi-partite *qubit* states $|\phi_a\rangle$ given by:

$$|\phi_a\rangle \quad = \quad \cos\theta_a\, |00\rangle + \sin\theta_a\, |11\rangle,$$

as θ_a varies. (This in fact gives the best protocol with qubit states.)

Question 5. [5 marks] Suppose we replace the commitment states $|\psi_a\rangle$ in the strong coin-flipping protocol we saw in class by mixed states $\rho_a \in \mathrm{L}(\mathbb{C}^d \otimes \mathbb{C}^d)$ of arbitrary dimension d. Explain what states and what final measurement by Bob would lead to a valid protocol. Then show that at least one part can cheat with probability at least 3/4, regardless of what commitment state is used.