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 4
Due: August 8, 2008

Question 1. [5 marks] Fix a distribution $p(x)$ for the random variable X, and a set of states $\{\sigma_x\}$ labeled by the outcomes of X. Let $\sigma = \sum_x p(x)\sigma_x$.

Fix n, and let $\Pi_{n,\epsilon}$ be the projection onto the strongly typical subspace of σ.

Let $x_i, \cdots, x_n$ be the outcome of n draws of X that is strongly typical, and $\sigma_{x^n} = \sigma_{x_1} \otimes \cdots \sigma_{x_n}$.

Show that $\text{Tr}(\sigma_{x^n}\Pi_{n,\epsilon}) \geq 1 - \delta_n$ for some small $\delta_n \to 0$. You can assume an AEP for strongly (frequency) typical sets analoguous to the one for (entropy) typical sets.

Question 2. Let $\mathcal{N}$ be a TCP map. Let $\chi(\mathcal{N}) = \sup_{\mathcal{E}} S(\sum_x p_x \mathcal{N}(\rho_x)) - \sum_x p_x S(\mathcal{N}(\rho_x))$ where the supremum is over the input ensemble $\mathcal{E} = \{p_x, \rho_x\}$.

(a) [5 marks] Show that the optimal ensemble can be choosen to consist of only pure states.

(b) **(Bonus)** Show that the optimal ensemble is finite, and contains no more than d^2 states if the input and output dimensions of $\mathcal{N}$ are both equal to d.

Hint: The following fact due to Davies and Caratheodory is relevant.

Let $P = \{A \geq 0, \text{tr}(A) = 1\}$. Let Y be the set of all probability measures of finite support on points in P. The set Y itself is compact and convex. Any extreme point of Y is a probability measure whose support has $\leq (1 + \dim P)$ points.

Question 3. [5 marks] (Entanglement concentration) Let Alice and Bob share n copies of $a|0\rangle + b|1\rangle$ and they want EPR pairs (ebits). Let $E = H(\{|a|^2, |b|^2\})$.

Show that there is a local operation followed by 1-bit of classical communication in each direction that enables $\geq n(E - \eta_n)$ ebits to be obtained with fidelity $\geq 1 - \zeta_n$. For each n, upper bound η_n and ζ_n in terms of the ϵ_n, δ_n in the AEP.

If they can communicate a little more (but in an amount sublinear in n), how can they create a probabilistic amount of exact ebits?

Question 4. [5 marks] Suppose that Alice and Bob share M EPR pairs, and each measures the their half for error syndrome for a CSS code C constructed out of classical codes $\{0\} \subseteq C_2 \subseteq C_1 \subseteq \mathbb{Z}_2^M$. Show that they both get the same uniformly random outcome $x \in \mathbb{Z}_2^M / C_1$ and $z \in \mathbb{Z}_2^M / C_2^\perp$, and the resulting state is the maximally entangled state in the subspace $C_{x,z} \otimes C_{x,z}$.

Question 5. [5 marks] Suppose an urn contains $3n$ red balls and n green balls. You pick $2n$ balls uniformly at random from the urn, without replacement. Prove that the probability that you pick fewer than $(3/2 - \nu)n$ red balls is exponentially small in $\nu^2 n$.