COMP-649A 2005 Homework set #3
Due Tuesday November 22, 2005 in class at 14h35

Approximate encryption

In the next few question, $\mathcal{E}(\rho)$ is an approximate quantum cipher ($i.e$ $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_\alpha < \epsilon$ for all ρ) and if ρ is an n qubit state, then the key has length $n + o(n)$.

1 Question #1

Show that an ϵ-approximate quantum cipher (according to the trace distance) destroys classical correlation. In other words let $\rho = \sum_i \varphi_i^A \otimes \psi_i^B$ be a separable state and $\mathcal{E}$ and ϵ-approximate cipher. Show

$$\left\|(\mathcal{E} \otimes \mathbb{I})(\rho^{AB}) - \frac{\mathbb{I}}{2^n} \otimes \rho^B\right\|_{tr} \leqslant \epsilon.$$

2 Question #2

Show that if there exist entanglement between the system A and the system B, then the above equation is not true.
(Hint : You may use the maximally entangle state and a rank argument to bootstrap).

3 Question #3

Assuming the stronger definition of an ϵ-approximate quantum cipher (($i.e$ $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_\infty < \epsilon$ for all ρ)) (key size is the same), Prove that a LOCC POVM can not see correlation between system A and system B. So if $M = \{M_i\}$ is a LOCC POVM and $p_i \triangleq \mathrm{tr}(M_i(R \otimes \mathbb{I})(\Phi))$ (where $|\Phi\rangle = \sum_i |i\rangle\,|i\rangle$)and $q_i \triangleq \mathrm{tr}\big(M_i \frac{\mathbb{I}}{2^{2n}}\big)$ then $\|p - q\| \leqslant \epsilon$. Hint :

1. for all i M_i has the form $M_i^A \otimes M_i^B$,
2. $M_i^B \mathrm{tr}\big(M_i^B\big) = {M_i^B}^2$, it works for the A system too (two hints in one),
3. $(\mathbb{I} \otimes M_i^B)\Phi(\mathbb{I} \otimes M_i^B) = \frac{1}{2^n} {M_i^B}^T \otimes M_i^B$

4 Question #4

Prove the hint of the previous question.

5 Question #5

Prove the more general statement : let $M = \{M_i\}$ is a LOCC POVM and $p_i \triangleq \operatorname{tr}\big(M_i(R \otimes \mathbb{I})(\rho^{AB})\big)$ and $q_i \triangleq \operatorname{tr}\big(M_i \frac{\mathbb{I}}{2^n} \otimes \rho^B\big)$ then $\|p - q\| \leqslant \epsilon$.

6 Question #6

A classical $[n, k, d]_Q$ code is a linear subspace of dimension k of length n vectors of $\mathbb{F}_Q$-components such that for any two distinct codewords c_1, c_2 we have that c_1 differs in at least d (out of n) positions from c_2. Let $\mathbb{F}_q$ be a subfield of $\mathbb{F}_Q$ such that $q = p^m$ and $Q = p^M$ for some prime p and integers $m < M$. An $[n, k, d]_Q$ code contains p^{kM} codewords (it is an $(n, Q^k, d)_Q$ linear code). If it contains only q codewords associated to the information words of $\mathbb{F}_q$ then the resulting code will be an $[n, m/M, d]_Q$ code (it is an $(n, q, d)_Q$ linear code). Since $m < M$ this code has fractional dimension, and it is linear only over the small field $\mathbb{F}_q$, not over $\mathbb{F}_Q$. Note that despite the fact that the fractional codes are normal regular codes on the smaller field, the error model is on elements of the larger field and thus we cannot speak of the code in the small field alone.

Stabilizer QECCs encoding k Q-dimensional registers in n Q-dimensional registers with quantum distance d (i.e., they are capable of correcting $\lfloor (d-1)/2 \rfloor$ general errors) are conventionally denoted with the notation $[[n, k, d]]_Q$, or $((n, Q^k, d))_Q$ for nonstabilizer codes. As in the classical case, we may define stabilizer QECCs with fractional dimension $[[n, m/M, d]]_Q$ to be $((n, q, d))_Q$ stabilizer codes.

Question: Prove that for any field size Q and any (fractional or integer) dimension κ if we have an $[[n, \kappa, d]]_Q$ Stabilizer QECC it corrects d erasures. Conclude that this implies that no (fractional or integer dimensional) QECC of length n can fix more than $n/4$ arbitrary errors, regardless of the dimension of the coding Hilbert space.