COMP-649B 2009 Homework set #3

Due Monday April, 20 2009

A. Non-Universality…

Let $\varepsilon(n)>0$ be some information bound (function). Assume that we would like to use an n-bit key $S = (S_1, \ldots, S_n)$ as a one-time pad to encrypt an n-bit message $M = (M_1, \ldots, M_n)$. Furthermore, assume that an adversary is interested in the n^{th} bit M_n of the message, but already knows the first $n-1$ bits $M_1, \ldots, M_{n-1}$. Upon observing the ciphertext, the adversary can easily determine the first $n-1$ bits of S.

[15%] • Show that the adversary can choose a random variable W such that $I(W;S)<\varepsilon$ but such that she can determine the n^{th} bit S_n with certainty from W and $S_1, \ldots, S_{n-1}$.

[5%] • What is the smallest information bound $\varepsilon(n)$ for which you can solve the above question ?

B. Quantum Secret Sharing…

[10%] • Show that an $[[n,k,d]]$ quantum error-correcting code can be used as a Quantum Secret Sharing scheme with n shares $s_1, s_2, \ldots, s_n$ such that fewer than A shares contain no information about the secret, whereas B or more shares are always enough to reconstruct the secret.

[10%] • Establish the bounds A and B as a function of n, k and d.

(If you find the general case too difficult, restrict your proof to **CSS** codes, for ½ the credits.)

[10%] • Find some **QECC** family such that $B=A+1$.

C. Code Equivalence (EQ)

Let G and G' be generator matrices of two linear codes C and C'. We say that codes C and C' are *equivalent* if there exists a permutation π of the columns of G such that $\pi(G)$ and G' generate the exact same linear subspace.

[15%] • Give a Zero-Knowledge protocol for the language **EQ** of all pairs of generating matrices of equivalent codes.

[15%] • Give an Interactive Proof for the complement language **Non-EQ**.

D. Quantum Linear Codes…

As far as I can tell, this problem leads to a genuinely original characterization of some Quantum Codes. We are about to define a notion of Quantum Linear Codes. For this exercise, we will focus on binary codes but it could be generalized easily to arbitrary fields, replacing the C-NOT gates by arbitrary ADDITION gates in the field.

A pair of n-qubit pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ are linearly compatible if there exists a pure state $|\phi_1\rangle$ such that $\text{C-NOT}^{\otimes n}(|\psi_0\rangle\otimes|\psi_1\rangle) = |\psi_0\rangle\otimes|\phi_1\rangle$.

[10%]
[5%]

1) Show that the code-words of a **CSS** code C form a set of linearly compatible states.
2) Show that for all $|\psi_0\rangle,|\psi_1\rangle\in C$, the corresponding $|\phi_1\rangle\in C$ as well.

A state $|\zeta\rangle$ is called the *zero-state* if it is such that for any linearly compatible state $|\psi\rangle$ we have $\text{C-NOT}^{\otimes n}(|\zeta\rangle\otimes|\psi\rangle) = |\zeta\rangle\otimes|\psi\rangle$.

[5%]

3) Identify the *zero-state* of a **CSS** code.

Let's define a basis spanning a linear sub-space of quantum states. A *basis* $|\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_k\rangle$ is a set of linearly compatible states. Intuitively, the *Span* of a basis is the set of all states that we can reach by linearly combining the states of the basis. We formally define the Span of a set of states recursively as follows:

$$\text{SPAN}(\ |\beta_0\rangle\ ) := \{\ |\zeta\rangle, |\beta_0\rangle\ \}$$

$$\text{SPAN}(\ |\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_k\rangle\ ) := \{\ |\psi\rangle \mid \text{there exists a } |\phi\rangle\in\text{SPAN}(\ |\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_{k-1}\rangle\ ) \text{ such that } \text{C-NOT}^{\otimes n}(|\beta\rangle\otimes|\phi\rangle) = |\beta\rangle\otimes|\psi\rangle, \text{ for either } |\beta\rangle = |\zeta\rangle \text{ or } |\beta_k\rangle.\}$$

[15%]

4) Show that for any CSS code C of dimension k, there exist k states $|\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_{k-1}\rangle$ such that $C = \text{SPAN}(\ |\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_{k-1}\rangle\ )$.

We define a Quantum Linear Code of size n and dimension k to be the Span of a set of k linearly compatible independent states $|\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_{k-1}\rangle$. (By independent we mean that for all index i, $|\beta_i\rangle\notin\text{SPAN}(\ |\beta_0\rangle,|\beta_1\rangle,\ldots,|\beta_{i-1}\rangle\ )$).

[+25%]

5) [**]Show that the sets of Linear Quantum Codes and Stabilizer Codes are indeed the same. Alternatively, find a Stabilizer Code that fails to satisfy one of the above 4 properties.

The proposed approach is to repeat the above four sub-questions with general Stabilizer Codes and proving that Linear Quantum Codes can always be defined by a Stabilizer.

[**] I have not yet proved this part, so we are all together into this …