COMP-649B 2009 Homework set #3

Due Tuesday April, 14 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.

• 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 $S_1, \ldots, S_{n-1}$.

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

B. Quantum Secret Sharing…

• 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.

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

(If you find the general case too difficult, prove the same things for CSS codes, for ½ the credits.)

• 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.

• Give a Zero-Knowledge protocol for the language EQ of all pairs of generating matrices of equivalent codes.

• Give an Interactive Proof for the complement language Non-EQ.