Exercise 4

February, 2006

1. Recall that a *character* of a group is a continuous homomorphism from that group to $C^{\times}$. Show that for any finite group G, there are at most $|G|$ different characters. Are there always exactly $|G|$ characters? (Hint: consider S_3.)

2. The Hadamard encoding of a string of n bits is a string of 2^n bits, consisting of the evaluation of all possible n-bit linear functionals on the input string.

   (a) What is the distance between any two words in the Hadamard encoding?

   (b) What is the distance of a given $f : \{1, -1\}^n \to \{0, 1\}$ from its closest codeword?

   (c) Show directly that the radius of the code (i.e., the distance from an arbitrary word to its closest codeword) is at most 1/2.

   (d) What is the orthogonal code to the Hadamard code for $n = 2$?

   (e) Assume that a noise demon changes every bit in a string with probability ϵ per bit. If we use the Hadamard code to encode our data before transmission, what is our decoding procedure? What is the probability (a good bound is sufficient) that a given transmission will be decoded correctly?

3. Let C be a linear code and $C^{\perp}$ orthogonal to it. Let $x, y \in \mathbb{R}$, and define $f, g : \{0, 1\}^n \to \mathbb{R}$ as follows: $f = 1_C, g(w) = x^{|w|} y^{n-|w|}$, where $|w|$ is the number of 1s in w.

   (a) Calculate $\hat{f}$.

   (b) Calculate $\hat{g}$.

   (c) Use Parseval's identity to prove the MacWilliams identity:

   $$P_C(x, y) = \frac{|C|}{2^n} P_{C^{\perp}}(y - x, y + x)$$

   where

   $$P_C(x, y) = \sum_{w \in C} x^{|w|} y^{n-|w|}$$

   Verify the identity by applying it to $C^{\perp}$.