CCS Discrete II	Professor: Padraic Bartlett

Homework 2: More Error-Correcting Codes

Due Friday, Week 2 — *UCSB 2015*

Do **three** of the **six** problems below! Prove all of your claims.

1. Here's a fun problem from a UCSB Ph.D. student[1] from their dissertation:

   Question. You and two friends have been captured by eeeeevil logicians! They tell you ahead of time about the following puzzle they have for you:

   - You will all be led into a locked room.
   - Each person will have a hat placed on their head; hats are either black or white, and randomly decided for each person by flipping a fair coin.
   - No one can see their own hat.
   - Each person can see other people's hats.
   - You and your friends cannot communicate once in the room.
   - When the guards say so, you and your friends must all either guess the color of their own hat, or say "pass."
   - If at least one person guesses correctly and no one is incorrect, you're free!
   - If anyone guesses incorrectly, you are sad/eaten by bears.

   Find a strategy that insures that on average, you are not eaten by bears three-quarters of the time.

2. A q-ary length n code C is called **linear** if the sum of any two codewords in C, thought of as elements in $(\mathbb{Z}/q\mathbb{Z})^n$, is also a codeword in C.

   (a) Find a linear code.

   (b) Find a nonlinear code.

   (c) Is the Hamming $[7, 4]$ code from problem set 1 linear?

3. A q-ary length n code C is called **perfect** if there is some integer t such that for any element $\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n$, there is a unique word in C within Hamming distance t of $\mathbf{x}$.

   (a) Find a perfect code

   (b) Find a nonperfect code.

   (c) Is the Hamming $[7, 4]$ code from problem set 11 perfect?

[1] Todd Ebert, 1998. The silly framing is me.

4. A **Hadamard matrix** is the following object: a $n \times n$ matrix, with entries all ± 1, such that all of the columns are orthogonal[2]. For example,

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

is a Hadamard matrix.

   (a) For any $n = 2^k$ for some k, find a Hadamard matrix.

   (b) Take the columns of any $n \times n$ Hadamard matrix, and replace the -1's with 0's. This gives you a binary code, all of whose codewords are length n. What is the distance of this code? What is the information rate? (Fun fact: we used these codes to communicate with Mariner 9, the first spacecraft to orbit another planet!)

5. Prove that $A_q(n, d) \leq q^{n+1-d}$.

6. In class, I claimed that we can assume that the codeword $\overbrace{000\ldots0}^{n \text{ zeroes}}$ is in any of our codes. Justify this claim as follows: given any base q, define a **Hamming-distance-preserving map** $\varphi : (\mathbb{Z}/q\mathbb{Z})^n \to (\mathbb{Z}/q\mathbb{Z})^n$ as any map with the following property:

   - For any two codewords $w_1, w_2 \in (\mathbb{Z}/q\mathbb{Z})^n$, we have that $d(w_1, w_2) = d(\varphi(w_1), \varphi(w_2))$.

   (a) For $q = 2, n = 4$, create a Hamming-distance-preserving map that is not the identity.

   (b) Prove that any Hamming-distance-preserving map is a bijection.

   (c) For any code C, let $\varphi(C)$ denote the code given by $\{\varphi(w) \mid w \in C\}$. Prove that if C is a code with $d(C) = k$, then $d(\varphi(C))$ is equal to k as well.

   (d) Show that for any code C, there is a Hamming-distance-preserving map φ that sends one codeword of C to the all-zero codeword $\overbrace{000\ldots0}^{n \text{ zeroes}}$.

[2] Two vectors $(a_1, a_2, \ldots a_n), (b_1, b_2, \ldots b_n)$ are called **orthogonal** if the sum $\sum_{k=1}^{n} a_k b_k$ is equal to 0. For example $(1, -3)$ and $(6, 2)$ are a pair of orthogonal vectors.