Math/CS 103	Professor: Padraic Bartlett

Handout 12: Error-Correcting Codes

Due Friday, Week 7 — *UCSB 2014*

Pick **two** of the **three** problems below, and solve them!

1. 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. Find a linear code. Find a nonlinear code. Is the Hamming $[7,4]$ code from problem set 11 linear?

2. 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 $\mathbf{x}$. Find a perfect code. Find a nonperfect code. Is the Hamming $[7,4]$ code from problem set 11 perfect?

3. A **Hadamard matrix**, which you may remember from last quarter, is the following object: a $n\times n$ matrix, with entries all ± 1, such that all of the columns are orthogonal. 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!)