Math 567: Introduction to Coding Theory

Homework 3: Due Friday, March 1

Problem 1.1. Show that the Hamming distance $d(,)$ on $\mathbb{F}_q^n$ satisfies the following properties.

1. $d(x, y) = 0$ if and only if $x = y$.
2. $d(x, y) = d(y, x)$ for all $x, y \in \mathbb{F}_q^n$.
3. $d(x, z) \leq d(x, y) + d(y, z)$ for all $x, y, z \in \mathbb{F}_q^n$.

Problem 1.2. Consider the Hamming $[7, 4]$ code that we discussed in class.

1. List all of the codewords of this code.
2. What is the rate of this code?
3. The following message was encoded using the Hamming $[7, 4]$ code. Locate and correct all errors:

   $$0011110 \qquad 0111100 \qquad 0001111 \qquad 0000011.$$

   (If I have not made any mistakes these should correspond to the first 4 digits of the binary expansion of e.)

Problem 1.3. Prove that the rows of an $(n - k) \times n$ parity check matrix H (associated to a linear $[n, k]$ code $\mathcal{C}$) are linearly independent. (Hint: Consider the linear transformation from $\mathbb{F}_q^n$ to $\mathbb{F}_q^{n-k}$ given by $x \mapsto Hx^T$. What is the kernel of this linear transformation? What is its rank?)

Problem 1.4. Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Let $\mathcal{C}_e$ be the set of codewords $x = (x_1, \ldots, x_n)$ of $\mathcal{C}$ with sum of coordinates zero; that is, $\sum_{i=1}^n x_i = 0$. Show that either $\mathcal{C} = \mathcal{C}_e$ or $\mathcal{C}_e$ is an $[n, k - 1]$ subcode of $\mathcal{C}$.

Problem 1.5. Let H be an Hadamard matrix of order N. Show that the rows and columns of H are pairwise orthogonal.