Problem Set 4

Information and Coding Theory

March 14, 2021

Clayton Seitz

Problem 0.1. *This is the first problem*

Solution.

$$\begin{aligned}\Delta(C) &= \min_{x_1,x_2\in C}\Delta(x_1,x_2)\\ &= \min_{x_1,x_2\in C}\Delta(0,x_2-x_1)\\ &= \min_{x\in C}\mathbf{wt}(x)\end{aligned}$$

Since the code is linear, $x_2 - x_1 \in C$. Now, we consider the parity check matrix $H \in \mathbb{F}_2^{r\times n}$ where $n = 2^r - 1$. We will find the dimension, block length, and distance for such a code. First, the dimension of the code $\dim(C)$ is $r+1$ since the rank of H is r. The block length is then 2^{r+1} and the distance is 3. Now, consider the Hamming code $C : \mathbb{F}_2^k \to \mathbb{F}_2^n$ which is formally defined as the set of x in the null space in of the parity check matrix:

$$C = \{x \in \mathbb{F}_2^n | Hx = 0\}$$

where $H \in \mathbb{F}_2^{k\times n}$ is the parity check matrix. We can also define the dual code $C^\perp$ to be the code with generator matrix H^T and parity check matrix G^T.

To see why this is possible, we will use the fact that we have defined our code C to be the vectors x that lie in the null space of the parity matrix H. Now, the definition of our code requires that $H(x) = H(G(w)) = 0$ which means that the generator matrix G is a matrix with columns equal to the basis vectors of the null space of H i.e. $HG = 0$. This is equivalent to saying that the columns of H^T form the basis of the null space of G^T:

$$HG = 0 \iff G^T H^T = 0$$

Therefore H^T can be viewed as the generator matrix and G^T the parity check matrix for the dual code $C^{\perp}$.

$\blacksquare$