

# M460 Information and Coding Theory

## homework sheet # 3

Select a sufficient number of problems from the following list to work on:

### Problem # 1

Evaluate the minimum distances of the binary codes which are generated by

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

### Problem # 2

Compute coset leaders for the binary code generated by

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Decode the vectors  $(1, 1, 0, 1, 0, 0)$  and  $(1, 1, 1, 1, 1, 1)$ .

### Problem # 3

A linear code  $C$  is self-orthogonal if and only if  $\langle c, c' \rangle = 0$  for all  $c, c' \in C$ . Show that  $C$  is self-dual (i.e.,  $C = C^\perp$ ) if and only if  $C$  is self-orthogonal and  $C$  is of dimension  $k = n/2$  (and hence  $n$  is even).

### Problem # 4

Let  $C$  be a binary, self-orthogonal code.

- Show that each word of  $C$  is even and that  $C^\perp$  contains the all-one vector  $\mathbf{1}$ .
- Assume in addition that the length  $n$  of  $C$  is odd and that the dimension of  $C$  is  $(n-1)/2$ . Show that

$$C^\perp = C \cup (\mathbf{1} + C).$$

### Problem # 5

Show that a code with check matrix  $H = (I_k \mid A)$  is self-dual if and only if  $A$  is a square matrix with  $A \cdot A^\top = -I_k$ .

### Problem # 6

Define the “intersection” of two binary vectors  $u$  and  $v$  to be the vector

$$u \wedge v : (u_0v_0, \dots, u_{n-1}v_{n-1})$$

which has ones only where both  $u$  and  $v$  have ones. Also, let

$$u \vee v : (1 - (1 - u_0)(1 - v_0), \dots, 1 - (1 - u_{n-1})(1 - v_{n-1}))$$

be the “union” of  $u$  and  $v$ , i.e. the vector which is one if at least one of  $u$  or  $v$  is one. Show that

$$\text{wt}(u + v) = \text{wt}(u) + \text{wt}(v) - 2\text{wt}(u \wedge v) = \text{wt}(u \vee v) - \text{wt}(u \wedge v).$$

### Problem # 7

Show the following:

- If  $u, v \in \mathbb{F}_2^n$ , then  $\langle u, v \rangle \equiv \text{wt}(u \wedge v) \pmod{2}$  (where  $u \wedge v$  is as in the previous problem).
- If  $u \in \mathbb{F}_2^n$ , then  $\langle u, u \rangle \equiv \text{wt}(u) \pmod{2}$ .
- If  $u \in \mathbb{F}_3^n$ , then  $\langle u, u \rangle \equiv \text{wt}(u) \pmod{3}$ .

### Problem # 8

A  $(n, k, d, q)$  is said to be perfect if the balls of radius  $e = \lfloor (d-1)/q \rfloor$  cover the whole Hamming space  $H(n, q)$ . Show that this is equivalent to

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i = q^{n-k}.$$

Deduce that

$$\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} \binom{n}{i} (q-1)^i \leq q^{n-k}$$

for any linear code. Is the binary  $(7, 4)$ -Hamming code perfect?

### Problem # 9

How many one-dimensional subspaces does the vector space  $\mathbb{F}_q^n = H(n, q)$  have?

### Problem # 10

Let  $H$  be a matrix whose columns form a system of representatives of the one-dimensional subspaces of  $\mathbb{F}_q^m$ . The code whose check matrix is  $H$  is called  $m$ -th order  $q$ -ary Hamming code. What are its parameters? Is it a perfect code?

### Problem # 11

Let  $\mathcal{C}$  be a linear  $(n, k, d)$  code. Define the parity extension of  $\mathcal{C}$  to be

$$P(\mathcal{C}) := \{(c_0, \dots, c_{n-1}, c_n) \mid (c_0, \dots, c_{n-1}) \in \mathcal{C}, c_n = -\sum_{i=0}^{n-1} c_i\}$$

Compute the minimum distance of  $P(\mathcal{C})$  (Hint: distinguish cases according to whether  $d$  is even or odd).

due Monday, April 2.