

Work on these questions by yourself !!  
 You can ask only me for help/hints.  
 Hand in the questions with your answers.

1. (15pts) Let  $C$  be a linear code of minimum weight  $2t$ . Prove that  $C$  has a coset containing at least two words of weight  $t$ .
2. (20pts) Let  $C$  be a binary linear code of length  $n$  and  $B$  the set of all codewords in  $C$  of even weight.
  - (a) (5pts) Prove that  $B$  is a binary linear code of length  $n$ .
  - (b) (10pts) If  $\mathbf{x} \in C$  is a codeword of odd weight, prove that  $B + \mathbf{x}$  is the set of all codewords in  $C$  of odd weight.
  - (c) (5pts) Prove that either all codewords in  $C$  have even weight or exactly half of the codewords in  $C$  have even weight.

3. (25pts) Let  $C_1$  be an  $[n_1, k_1, d_1]$ -code over  $GF(q)$  and  $C_2$  an  $[n_2, k_2, d_2]$ -code over  $GF(q)$ . Consider the code

$$C := \{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in C_1 \text{ and } \mathbf{y} \in C_2\}$$

- (a) (5pts) Prove that  $C$  is a linear code of length  $n_1 + n_2$  over  $GF(q)$ .
- (b) (15pts) Let  $\{\mathbf{x}_1, \dots, \mathbf{x}_{k_1}\}$  be a basis for  $C_1$  and  $\{\mathbf{y}_1, \dots, \mathbf{y}_{k_2}\}$  a basis for  $C_2$ . Prove that

$$\{(\mathbf{x}_1, \mathbf{0}), \dots, (\mathbf{x}_{k_1}, \mathbf{0}), (\mathbf{0}, \mathbf{y}_1), \dots, (\mathbf{0}, \mathbf{y}_{k_2})\}$$

is a basis for  $C$ .

- (c) (5pts) Prove that  $d(C) = \min\{d_1, d_2\}$ .
4. (25pts) This exercise is about Reed-Muller codes.
  - (a) (7pts) Prove that  $\mathbf{1} \in R(1, m)$  for all  $lm \geq 1$ .
  - (b) (18pts) Let  $m \geq 1$  and  $0 \leq r_1 \leq r_2 \leq m$ . Prove that  $R(r_1, m) \subseteq R(r_2, m)$ .  
 Hint: Let  $0 \leq r < m$ . Prove that  $R(r, m) \subseteq R(r + 1, m)$ .
5. (20pts) We put  $GF(3) = \{0, 1, 2\}$  (so working modulo 3). It is given that  $x^2 + x + 2$  is primitive over  $GF(3)$ . Define  $\alpha$  by  $\alpha^2 + \alpha + 2 = 0$ . Set up a table for  $GF(9)$  containing the polynomial expression  $a_1\alpha + a_0$ , the ternary expression  $a_1a_0$  and the exponential form  $\alpha^i$  for each element of  $GF(9)$ .

6. (20pts) Find all the irreducible factors of  $x^8 - 1$  over  $GF(3) = \{0, 1, 2\}$ .
7. (20pts) This exercise is about cyclic codes of length 19 over  $GF(7)$ .
- (5pts) List the degrees of all the irreducible factors of  $x^{19} - 1$  over  $GF(7)$ . You can label the factors by  $g_1(x), g_2(x), \dots$
  - (5pts) How many cyclic codes of length 19 over  $GF(7)$  are there?
  - (5pts) Write (in terms of  $g_1(x), g_2(x), \dots$ ) the generator polynomial of a cyclic code of length 19 over  $GF(7)$  of dimension at least six that can correct at least four errors.
  - (5pts) Write (in terms of  $g_1(x), g_2(x), \dots$ ) the generator polynomial of cyclic code of length 19 over  $GF(7)$  of dimension thirteen that is not a BCH-code.
8. (55pts) Let  $\alpha$  be the primitive element of  $GF(16)$  as defined in the table for  $GF(16)$  in the notes. Then  $GF(4) = \{0, 1, \alpha^5, \alpha^{10}\}$  is a subfield of  $GF(16)$ . Consider the BCH-code of length 15 over  $GF(4)$  with generator polynomial  $\text{lcm}(m_{\beta^5}(x), m_{\beta^6}(x), m_{\beta^7}(x), m_{\beta^8}(x)m_{\beta^9}(x), m_{\beta^{10}}(x))$ .
- (5pts) What are the dimension and designed distance of this code?
  - (50pts) Suppose we receive the word

$$\mathbf{y} = 010\alpha^5 00000000000$$

- (25pts) Use the Peterson-Gorenstein-Zierler decoding algorithm to decode  $\mathbf{y}$ .
- (25pts) Use the Key Equation to decode  $\mathbf{y}$ .

Extra Credit (20pts) : Let  $C$  be the binary linear code of length 9 defined by

$x_1x_2x_3x_4x_5x_6x_7x_8x_9 \in C$  if and only if every row and every column of the matrix

$$\begin{bmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{bmatrix}$$

contains an even number of ones.

Find  $\dim(C)$  and  $d(C)$ .