

1. The codewords in the first order Reed-Muller code  $R(1, 3)$  are of the form

$$x_1x_2 \dots x_7x_8 = [ a_3 \ a_2 \ a_1 \ a_0 ] G(1, 3)$$

- (a) Find the parity check sums for  $a_1$ ,  $a_2$  and  $a_3$ .  
 (b) Decode 10000011.  
 (c) Decode 10101010.
2. Consider the binary matrix

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Show that  $G$  is a generator matrix for the second order Reed-Muller code  $R(2, 3)$ .

3. Explain the probabilities on page 33 in the notes. First write your answers in terms of a general symbol-error-probability  $p$ . Then evaluate your answers (you will need a computer to find 99.99%).
4. It is given that  $f(x) = x^4 + x + 1$  is irreducible and primitive over  $GF(2)$ . Define  $\alpha$  by  $f(\alpha) = 0$ .
- (a) Set up a table for  $GF(16)$  containing the binary, exponential and polynomial representation of every element in  $GF(16)$ .
- (b) Solve for  $x$  and  $y$ :  $\begin{cases} x + \alpha^7y = \alpha^{10} \\ \alpha^2x + y = \alpha^5 \end{cases}$ . Write all elements of  $GF(16)$  in exponential form.
- (c) Find the quotient and remainder of  $x^5 + \alpha^2x^4$  divided by  $x^2 + \alpha x + \alpha^2$ . Write all elements of  $GF(16)$  in exponential form.
5. Let  $\beta$  be a primitive 5-th root of unity in  $GF(16)$ . Then over  $GF(16)$ , we can factor  $x^5 - 1$  as

$$x^5 - 1 = (x - 1)(x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)$$

Let  $\alpha$  be defined as in Exercise 4. Write all elements of  $GF(16)$  in exponential form.

- (a) What are the choices for  $\beta$  in terms of  $\alpha$ ?
- (b) Use cyclotomic cosets to find the degrees of the irreducible factors of  $x^5 - 1$  over  $GF(2)$ .
- (c) Use the table from Exercise 4 to expand the appropriate combinations of  $x - 1$ ,  $x - \beta$ ,  $x - \beta^2$ ,  $x - \beta^3$  and  $x - \beta^4$  to get the irreducible factors of  $x^5 - 1$  over  $GF(2)$ .
- (d) We can view  $GF(4)$  as a subfield of  $GF(16)$ . Which elements of  $GF(16)$  form  $GF(4)$ ?
- (e) Use cyclotomic cosets to find the degrees of the irreducible factors of  $x^5 - 1$  over  $GF(4)$ .
- (f) Use the table from Exercise 4 to expand the appropriate combinations of  $x - 1$ ,  $x - \beta$ ,  $x - \beta^2$ ,  $x - \beta^3$  and  $x - \beta^4$  to get the irreducible factors of  $x^5 - 1$  over  $GF(4)$ .
6. Let  $\mathbb{F}, \mathbb{K}$  be fields such that  $\mathbb{F} \subseteq \mathbb{K}$  and  $\dim_{\mathbb{F}} \mathbb{K}$  is finite. Let  $\alpha \in \mathbb{K}$ .
- (a) Prove that there exists a monic non-zero polynomial  $f(x) \in \mathbb{F}[x]$  such that  $f(\alpha) = 0$ .
- (b) Let  $m(x)$  be a monic non-zero polynomial in  $\mathbb{F}[x]$  with  $m(\alpha) = 0$  of smallest degree. Why does  $m(x)$  exist? Prove that  $m(x)$  is unique and irreducible.
- (c) Let  $f(x) \in \mathbb{F}[x]$  with  $f(\alpha) = 0$ . Prove that  $m(x)$  divides  $f(x)$ .