

---



---

ESE 532  
HW #10 Solutions

---



---

**Problem 10.30**

To generate a (7,3) cyclic code we need a generator polynomial of degree  $7 - 3 = 4$ . Since (see Example 10.6.2))

$$\begin{aligned} p^7 + 1 &= (p + 1)(p^3 + p^2 + 1)(p^3 + p + 1) \\ &= (p^4 + p^2 + p + 1)(p^3 + p + 1) \\ &= (p^3 + p^2 + 1)(p^4 + p^3 + p^2 + 1) \end{aligned}$$

either one of the polynomials  $p^4 + p^2 + p + 1$ ,  $p^4 + p^3 + p^2 + 1$  can be used as a generator polynomial. With  $g(p) = p^4 + p^2 + p + 1$  all the codeword polynomials  $c(p)$  can be written as

$$c(p) = X(p)g(p) = X(p)(p^4 + p^2 + p + 1)$$

where  $X(p)$  is the message polynomial. The following table shows the input binary sequences used to represent  $X(p)$  and the corresponding codewords.

Input	$X(p)$	$c(p) = X(p)g(p)$	Codeword
000	0	0	0000000
001	1	$p^4 + p^2 + p + 1$	0010111
010	$p$	$p^5 + p^3 + p^2 + p$	0101110
100	$p^2$	$p^6 + p^4 + p^3 + p^2$	1011100
011	$p + 1$	$p^5 + p^4 + p^3 + 1$	0111001
101	$p^2 + 1$	$p^6 + p^3 + p + 1$	1001011
110	$p^2 + p$	$p^6 + p^5 + p^4 + p$	1110010
111	$p^2 + p + 1$	$p^6 + p^5 + p^2 + 1$	1100101

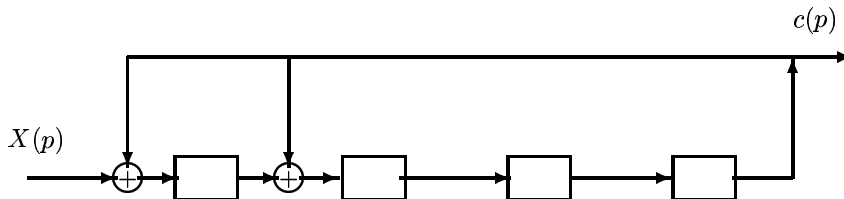
Since the cyclic code is linear and the minimum weight is  $w_{\min} = 4$ , we conclude that the minimum distance of the (7,3) code is 4.

**Problem 10.31**

Using Table 10.1 we find that the coefficients of the generator polynomial of the (15,11) code are given in octal form as 23. Since, the binary expansion of 23 is 010011, we conclude that the generator polynomial is

$$g(p) = p^4 + p + 1$$

The encoder for the (15,11) cyclic code is depicted in the next figure.



**Problem 10.32**

The  $i^{\text{th}}$  row of the matrix  $\mathbf{G}$  has the form

$$\mathbf{g}_i = [ 0 \ \cdots \ 0 \ 1 \ 0 \cdots 0 \ p_{i,1} \ p_{i,2} \ \cdots \ p_{i,n-k} ], \quad 1 \leq i \leq k$$

where  $p_{i,1}, p_{i,2}, \dots, p_{i,n-k}$  are found by solving the equation

$$p^{n-i} + p_{i,1}p^{n-k-1} + p_{i,2}p^{n-k-2} + \cdots + p_{i,n-k} = p^{n-i} \pmod{g(p)}$$

Thus, with  $g(p) = p^4 + p + 1$  we obtain

$$p^{14} \pmod{p^4 + p + 1} = (p^4)^3 p^2 \pmod{p^4 + p + 1} = (p + 1)^3 p^2 \pmod{p^4 + p + 1}$$



As it is observed from the table, the minimum weight of the code is 5 and since the code is linear  $d_{\min} = w_{\min} = 5$ .

3) The coding gain of the (10, 2) cyclic code in part 1) is

$$G_{\text{coding}} = d_{\min}R = 5 \times \frac{2}{10} = 1$$

**Problem 10.34**

1) For every  $n$

$$p^n + 1 = (p + 1)(p^{n-1} + p^{n-2} + \dots + p + 1)$$

where additions are modulo 2. Since  $p + 1$  divides  $p^n + 1$  it can generate a  $(n, k)$  cyclic code, where  $k = n - 1$ .

2) The  $i^{\text{th}}$  row of the generator matrix has the form

$$\mathbf{g}_i = [ 0 \quad \dots \quad 0 \quad 1 \quad 0 \quad \dots \quad 0 \quad p_{i,1} ]$$

where  $p_{i,1}$ ,  $i = 1, \dots, n - 1$ , can be found by solving the equations

$$p^{n-i} + p_{i,1} = p^{n-i} \pmod{p + 1}, \quad 1 \leq i \leq n - 1$$

Since  $p^{n-i} \pmod{p + 1} = 1$  for every  $i$ , the generator and the parity check matrix are given by

$$\mathbf{G} = \left( \begin{array}{ccc|c} 1 & \dots & 0 & 1 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 1 \end{array} \right), \quad \mathbf{H} = [ 1 \quad 1 \quad \dots \quad 1 \quad | \quad 1 ]$$

3) A vector  $\mathbf{c} = [c_1, c_2, \dots, c_n]$  is a codeword of the  $(n, n - 1)$  cyclic code if it satisfies the condition  $\mathbf{c}\mathbf{H}^t = 0$ . But,

$$\mathbf{c}\mathbf{H}^t = 0 = \mathbf{c} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} = c_1 + c_2 + \dots + c_n$$

Thus, the vector  $\mathbf{c}$  belongs to the code if it has an even weight. Therefore, the cyclic code generated by the polynomial  $p + 1$  is a simple parity check code.

**Problem 10.35**

1) Using the results of Problem 10.29, we find that the shortest possible generator polynomial of degree 4 is

$$g(p) = p^4 + p^2 + 1$$

The  $i^{\text{th}}$  row of the generator matrix  $\mathbf{G}$  has the form

$$\mathbf{g}_i = [ 0 \quad \dots \quad 0 \quad 1 \quad 0 \quad \dots \quad 0 \quad p_{i,1} \quad \dots \quad p_{i,4} ]$$

where  $p_{i,1}, \dots, p_{i,4}$  are obtained from the relation

$$p^{6-i} + p_{i,1}p^3 + p_{i,2}p^2 + p_{i,3}p + p_{i,4} = p^{6-i} \pmod{p^4 + p^2 + 1}$$

Hence,

$$\begin{aligned} p^5 \pmod{p^4 + p^2 + 1} &= (p^2 + 1)p \pmod{p^4 + p^2 + 1} = p^3 + p \\ p^4 \pmod{p^4 + p^2 + 1} &= p^2 + 1 \pmod{p^4 + p^2 + 1} = p^2 + 1 \end{aligned}$$

and therefore,

$$\mathbf{G} = \left( \begin{array}{cc|cccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right)$$

The codewords of the code are

$$\begin{aligned}\mathbf{c}_1 &= [ 0 \ 0 \ 0 \ 0 \ 0 \ 0 ] \\ \mathbf{c}_2 &= [ 1 \ 0 \ 1 \ 0 \ 1 \ 0 ] \\ \mathbf{c}_3 &= [ 0 \ 1 \ 0 \ 1 \ 0 \ 1 ] \\ \mathbf{c}_4 &= [ 1 \ 1 \ 1 \ 1 \ 1 \ 1 ]\end{aligned}$$

2) The minimum distance of the linear (6, 2) cyclic code is  $d_{\min} = w_{\min} = 3$ . Therefore, the code can correct

$$e_c = \frac{d_{\min} - 1}{2} = 1 \text{ error}$$

3) An upper bound of the block error probability is given by (see (10.5.23))

$$p_e = (M - 1)Q \left[ \sqrt{\frac{d_{\min} \mathcal{E}_s}{N_0}} \right]$$

With  $M = 2$ ,  $d_{\min} = 3$  and

$$\frac{\mathcal{E}_s}{N_0} = R_c \frac{\mathcal{E}_b}{N_0} = R_c \frac{P}{RN_0} = \frac{2}{6} \times \frac{1}{2 \times 6 \times 10^4 \times 2 \times 10^{-6}} = 1.3889$$

we obtain

$$p_e = Q \left[ \sqrt{3 \times 1.3889} \right] = 2.063 \times 10^{-2}$$

---

---