

**PROBLEMS**

- 6.1 Consider the Galois field  $GF(2^4)$  given by Table 2.8. The element  $\beta = \alpha^7$  is also a primitive element. Let  $g_0(X)$  be the lowest-degree polynomial over  $GF(2)$  that has

$$\beta, \beta^2, \beta^3, \beta^4$$

as its roots. This polynomial also generates a double-error-correcting primitive BCH code of length 15.

- Determine  $g_0(X)$ .
  - Find the parity-check matrix for this code.
  - Show that  $g_0(X)$  is the reciprocal polynomial of the polynomial  $g(X)$  that generates the (15, 7) double-error-correcting BCH code given in Example 6.1.
- 6.2 Determine the generator polynomials of all the primitive BCH codes of length 31. Use the Galois field  $GF(2^5)$  generated by  $p(X) = 1 + X^2 + X^5$ .
- 6.3 Suppose that the double-error-correcting BCH code of length 31 constructed in Problem 6.2 is used for error correction on a BSC. Decode the received polynomials  $r_1(X) = X^7 + X^{30}$  and  $r_2(X) = 1 + X^{17} + X^{28}$ .
- 6.4 Consider a  $t$ -error-correcting primitive binary BCH code of length  $n = 2^m - 1$ . If  $2t + 1$  is a factor of  $n$ , prove that the minimum distance of the code is exactly  $2t + 1$ . (*Hint:* Let  $n = l(2t + 1)$ . Show that  $(X^n + 1)/(X^l + 1)$  is a code polynomial of weight  $2t + 1$ .)
- 6.5 Is there a binary  $t$ -error-correcting BCH code of length  $2^m + 1$  for  $m \geq 3$  and  $t < 2^{m-1}$ ? If there is such a code, determine its generator polynomial.
- 6.6 Consider the field  $GF(2^4)$  generated by  $p(X) = 1 + X + X^4$  (see Table 2.8). Let  $\alpha$  be a primitive element in  $GF(2^4)$  such that  $p(\alpha) = 0$ . Devise a circuit that is capable of multiplying any element in  $GF(2^4)$  by  $\alpha^7$ .
- 6.7 Devise a circuit that is capable of multiplying any two elements in  $GF(2^5)$ . Use  $p(X) = 1 + X^2 + X^5$  to generate  $GF(2^5)$ .
- 6.8 Devise a syndrome computation circuit for the binary double-error-correcting (31, 21) BCH code.
- 6.9 Devise a Chien's searching circuit for the binary double-error-correcting (31, 21) BCH code.
- 6.10 Consider the Galois field  $GF(2^6)$  given by Table 6.2. Let  $\beta = \alpha^3$ ,  $l_0 = 2$ , and  $d = 5$ . Determine the generator polynomial of the BCH code that has

$$\beta^2, \beta^3, \beta^4, \beta^5$$

as its roots (the general form presented at the end of Section 6.1). What is the length of this code?

- 6.11 Let  $l_0 = -t$  and  $d = 2t + 2$ . Then we obtain a BCH code of designed distance  $2t + 2$  whose generator polynomial has

$$\beta^{-t}, \dots, \beta^{-1}, \beta^0, \beta^1, \dots, \beta^t$$

and their conjugates as all its roots.

- Show that this code is a reversible cyclic code.
- Show that if  $t$  is odd, the minimum distance of this code is at least  $2t + 4$ . (*Hint:* Show that  $\beta^{-(t+1)}$  and  $\beta^{t+1}$  are also roots of the generator polynomial.)