(e) Show that the probability of a 100-word message being correctly decoded by the standard array is at least .92. [Compare with part (b).]

16.3 BCH Codes

The Hamming codes in the last section have efficient decoding algorithms that correct all single errors. The same is true of the BCH codes* presented here. But these codes are even more useful because they correct multiple errors.

The construction of a BCH code uses a finite *ring* whose additive group is (isomorphic to) some $B(n)$. Each ideal in such a ring is a linear code because its additive group is (isomorphic to) a subgroup of $B(n)$. The additional algebraic structure of the ring provides efficient error-correcting decoding algorithms for the code.

The finite rings in question are constructed as follows. Let n be a positive integer and $(x^n - 1)$ the principal ideal in $\mathbf{Z}_2[x]$ consisting of all multiples of $x^n - 1$. The elements of the quotient ring $\mathbf{Z}_2[x]/(x^n - 1)$ are the congruence classes (cosets) modulo $x^n - 1$. By Corollary 5.5, the distinct congruence classes in $\mathbf{Z}_2[x]/(x^n - 1)$ are in one-to-one correspondence with the polynomials of the form

$$(*) \qquad a_0 + a_1x + a_2x^2 + \cdots a_{n-1}x^{n-1}, \qquad \text{with } a_i \in \mathbf{Z}_2.$$

Each such polynomial has n coefficients, and there are two possibilities for each coefficient. Hence $\mathbf{Z}_2[x]/(x^n - 1)$ is a ring with 2^n elements. Furthermore, the n coefficients $(a_0, a_1, a_2, \ldots, a_{n-1})$ of the polynomial $(*)$ may be considered as an element of the group $B(n) = \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2$.

THEOREM 16.12 *The function $f: \mathbf{Z}_2[x]/(x^n - 1) \to B(n)$ given by $f([a_0 + a_1x + a_2x^2 + \cdots a_{n-1}x^{n-1}]) = (a_0, a_1, a_2, \ldots, a_{n-1})$ is an isomorphism of additive groups.*

Proof Exercise 7. ∎

Theorem 16.12 shows that every ideal of $\mathbf{Z}_2[x]/(x^n - 1)$ can be considered as a linear code since it is (up to isomorphism) a subgroup of $B(n)$. In particular, if $g(x) \in \mathbf{Z}_2[x]$, then the congruence class (coset) of $g(x)$ generates a principal ideal I in $\mathbf{Z}_2[x]/(x^n - 1)$. The ideal I consists of all congruence classes of the form $[h(x)g(x)]$ with $h(x) \in \mathbf{Z}_2[x]$. BCH codes are of this type.

* The initials BCH stand for Bose, Chaudhuri, and Hocquenghem, who invented these codes in 1959–60.

In order to define a BCH code that corrects t errors, choose a positive integer r such that $t < 2^{r-1}$. Let $n = 2^r - 1$. Then $g(x)$ is determined by considering a finite field of order 2^r, as explained below.

EXAMPLE We let $t = 2$ and $r = 4$, so that $n = 2^4 - 1 = 15$. We shall construct a code in $\mathbf{Z}_2[x]/(x^{15} - 1)$ that corrects all double errors by finding an appropriate $g(x)$. To do this we need a field of order $2^4 = 16$.

The polynomial $1 + x + x^4$ is irreducible in $\mathbf{Z}_2[x]$ (Exercise 3). Hence $K = \mathbf{Z}_2[x]/(1 + x + x^4)$ is a field of order 16 by Theorem 5.9 (and the remarks after it). By Theorem 5.10, K contains a root α of $1 + x + x^4$. Using the fact that

$$1 + \alpha + \alpha^4 = 0, \qquad \text{and hence,} \qquad \alpha^4 = 1 + \alpha^*$$

we can compute the powers of α. For example, $\alpha^6 = \alpha^2\alpha^4 = \alpha^2(1 + \alpha) = \alpha^2 + \alpha^3$. Similarly, we obtain

$\alpha^1 = \alpha$	$\alpha^6 = \alpha^2 + \alpha^3$	$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$
$\alpha^2 = \alpha^2$	$\alpha^7 = 1 + \alpha + \alpha^3$	$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$
$\alpha^3 = \alpha^3$	$\alpha^8 = 1 + \alpha^2$	$\alpha^{13} = 1 + \alpha^2 + \alpha^3$
$\alpha^4 = 1 + \alpha$	$\alpha^9 = \alpha + \alpha^3$	$\alpha^{14} = 1 + \alpha^3$
$\alpha^5 = \alpha + \alpha^2$	$\alpha^{10} = 1 + \alpha + \alpha^2$	$\alpha^{15} = 1$

These elements are distinct and nonzero by Theorem 9.7. Therefore they are all the nonzero elements of K, and α is a generator of the multiplicative group of K.

To construct the polynomial $g(x)$, we first find the minimum polynomials of α, α^2, α^3, α^4 over $\mathbf{Z}_2$. By the construction of K, the minimal polynomial of α is $m_1(x) = 1 + x + x^4$. This polynomial $m_1(x)$ is also the minimal polynomial of α^2 and α^4; for instance, by the Freshman's Dream (Lemma 9.24),

$$\begin{aligned} m_1(\alpha^2) &= 1 + (\alpha^2) + (\alpha^2)^4 \\ &= 1^2 + (\alpha)^2 + (\alpha^4)^2 = (1 + \alpha + \alpha^4)^2 = 0^2 = 0. \end{aligned}$$

Verify that the minimum polynomial of α^3 is $m_3(x) = 1 + x + x^2 + x^3 + x^4$ (Exercise 5). The polynomial $g(x)$ is defined as the product $m_1(x)m_3(x)$, so that

$$\begin{aligned} g(x) &= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4) \\ &= 1 + x^4 + x^6 + x^7 + x^8 \in \mathbf{Z}_2[x]. \end{aligned}$$

* Remember, $1 = -1$ in $\mathbf{Z}_2$.

Let C be the ideal generated by $[g(x)]$ in $\mathbf{Z}_2[x]/(x^{15}-1)$. Then C is a code by Theorem 16.12. We shall see below that C is a (15,7) code that corrects all single and double errors.

Just what do the codewords of C look like? By Corollary 5.5, each congruence class in $\mathbf{Z}_2[x]/(x^{15}-1)$ is the class of a unique polynomial of the form

$$(**) \qquad a_0 + a_1x + a_2x^2 + \cdots + a_{13}x^{13} + a_{14}x^{14}, \qquad \text{with } a_i \in \mathbf{Z}_2.$$

So we shall denote the class by this polynomial.* When convenient, this polynomial will be identified (as in Theorem 16.12) with the element $a_0a_1a_2 \cdots a_{14} = (a_0, a_1, a_2, \ldots, a_{14})$ of $B(15)$. The codewords consist of the classes of polynomial multiples of $g(x)$. For example,

Codeword in polynomial form	*In B(15) form*
$g(x) = 1 + x^4 + x^6 + x^7 + x^8$	100010111000000
$xg(x) = x(1 + x^4 + x^6 + x^7 + x^8)$	
$= x + x^5 + x^7 + x^8 + x^9$	010001011100000
$(1 + x^6)g(x) = (1 + x^6)(1 + x^4 + x^6 + x^7 + x^8)$	
$= 1 + x^4 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{14}$	100010011010111

If $g(x)$ is multiplied by a polynomial $h(x)$ of degree ≥ 7, then the codeword $h(x)g(x)$ has degree ≥ 15 and is not of the form (**). For example, if $h(x) = x^8$, then

$$h(x)g(x) = x^8g(x) = x^8(1 + x^4 + x^6 + x^7 + x^8)$$
$$= x^8 + x^{12} + x^{14} + x^{15} + x^{16}.$$

The polynomial of the form (**) that is in the same class as $h(x)g(x)$ is the remainder when $h(x)g(x)$ is divided by $x^{15} - 1$ (see Corollary 5.5). Verify that

$$h(x)q(x) = (1 + x)(x^{15} - 1) + (1 + x + x^8 + x^{12} + x^{14}).$$

Hence $[f(x)g(x)]$ is the codeword $1 + x + x^8 + x^{12} + x^{14}$, or equivalently, 110000001000101.

The procedure in the example is readily generalized. If t is the number of errors the code should correct, let $n = 2^r - 1$, where r is chosen so that $t < 2^{r-1}$ (in the example, $t = 2$, $r = 4$). By Corollary 9.26, there is a finite field K of order 2^r. By Theorem 9.28, $K = \mathbf{Z}_2(\alpha)$, where α is a generator of

* This is analogous to what was done on pages 33–34, when we began writing elements (classes) in $\mathbf{Z}_n$ in the form k rather than $[k]$.

the multiplicative group of nonzero elements of K (and so has multiplicative order $2^r - 1 = n$). Let

$$m_1(x), m_2(x), m_3(x), \ldots, m_{2t}(x) \in \mathbf{Z}_2[x]$$

be the minimal polynomials of the elements

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t} \in K.$$

Let $g(x)$ be the product in $\mathbf{Z}_2[x]$ of the distinct polynomials on the list $m_1(x)$, $m_2(x), \ldots, m_{2t}(x)$.

The ideal C generated by $[g(x)]$ in $\mathbf{Z}_2[x]/(x^n - 1)$ is called the (primitive narrow-sense) **BCH code of length n and designed distance $2t + 1$ with generator polynomial** $g(x)$. So the code in the last example is a BCH code of length 15 and designed distance 5 $(=2 \cdot 2 + 1)$. If $g(x)$ has degree m, then Exercise 14 shows that the code C is an (n,k) code, where $k = n - m$.

THEOREM 16.13 *A BCH code of length n and designed distance 2t + 1 corrects t errors.*

Proof The proof requires a knowledge of determinants; see Lidl-Pilz [34; page 230] or Mackiw [35; page 60]. ∎

Theorem 16.13 shows that there are BCH codes that will correct any desired number of errors. More important, from a practical viewpoint, there are efficient algorithms for decoding large BCH codes.* A complete description of them would take us too far afield. But here, in simplified form, is the underlying idea of the error-correcting procedure.

Let C be a BCH code of designed distance $2t + 1$ and generator polynomial $g(x)$. By the definition of $g(x)$, each minimal polynomial $m_i(x)$ divides $g(x)$. Hence $g(\alpha^i) = 0$ for each $i = 1, 2, \ldots, 2t$. If $[f(x)]$ is a codeword in C, then $f(x) = h(x)g(x)$ for some $h(x)$, and therefore

$$f(\alpha^i) = h(\alpha^i)g(\alpha^i) = h(\alpha^i) \cdot 0 = 0.$$

Conversely, if $f(x) \in \mathbf{Z}_2[x]$ has every α^i as a root, then every $m_i(x)$ divides $f(x)$ by Theorem 9.6. This implies that $g(x) \mid f(x)$ (Exercise 8). Therefore

$$[f(x)] \text{ is a codeword if and only if } f(\alpha^i) = 0 \text{ for } 1 \leq i \leq 2t.$$

The decoder receives the word $a_0 a_1 \cdots a_k$ which represents the (class of) the polynomial

$$r(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k.$$

* This is one reason BCH codes are widely used. For example, the European and trans-Atlantic communication system uses a BCH code with $t = 6$ and $r = 8$. It is a (255,231) code that corrects six errors with a failure probability of only 1 in 16 million.

The decoder computes these elements of the field $K = \mathbb{Z}_2(\alpha)$:

$$r(\alpha), r(\alpha^2), r(\alpha^3), \ldots, r(\alpha^{2t}).$$

If all of them are 0, then $r(x)$ is a codeword by the remarks above. If certain ones are nonzero, the decoder uses them (according to a specified procedure) to construct a polynomial $D(x) \in K[x]$, called the **error-locator polynomial.** Since K is finite, the nonzero roots of $D(x)$ in K can be found by substituting each $\alpha^i \in K$ in $D(x)$].

If no more than t errors have been made, the nonzero roots of $D(x)$ give the location of the transmission errors. For instance, if α^7 is a root, then a_7 is incorrect in the received word $r(x)$; similarly if $\alpha^0 = 1$ is a root, then an error occurred in transmitting a_0.

If $D(x)$ has no roots in K or if certain of the $r(\alpha^i)$ are 0, so that $D(x)$ cannot be constructed, then more than t errors have been made. So the decoder follows set procedures (omitted here) to choose arbitrarily a nearest codeword to $r(x)$.

EXAMPLE In the (15,7) BCH code of the previous example, suppose this word is received:

$$r(x) = x + x^7 + x^8 = 010000011000000.$$

Using the table on page 460 and the fact that $u + u = 0$ for every element u in K (Exercise 1), we have

$$r(\alpha) = \alpha + \alpha^7 + \alpha^8 = \alpha + (1 + \alpha + \alpha^3) + (1 + \alpha^2)$$
$$= \alpha^2 + \alpha^3 = \alpha^6.$$
$$r(\alpha^3) = \alpha^3 + (\alpha^3)^7 + (\alpha^3)^8$$
$$= \alpha^3 + \alpha^{21} + \alpha^{24} = \alpha^3 + \alpha^6 + \alpha^9$$
$$= \alpha^3 + (\alpha^2 + \alpha^3) + (\alpha + \alpha^3) = \alpha + \alpha^2 + \alpha^3 = \alpha^{11}.$$

Exercise 6 shows that

$$r(\alpha^2) = r(\alpha)^2 = (\alpha^6)^2 = \alpha^{12};$$
$$r(\alpha^4) = r(\alpha)^4 = (\alpha^6)^4 = \alpha^{24} = \alpha^9.$$

The error-locator polynomial is given by this formula (which is justified in Exercise 15):

$$D(x) = x^2 + r(\alpha)x + \left(r(\alpha^2) + \frac{r(\alpha^3)}{r(\alpha)}\right).$$

Using the table on page 460 we see that

$$D(x) = x^2 + \alpha^6 x + \left(\alpha^{12} + \frac{\alpha^{11}}{\alpha^6}\right) = x^2 + \alpha^6 x + (\alpha^{12} + \alpha^5)$$
$$= x^2 + \alpha^6 x + \alpha^{14}.$$

By substituting each of the nonzero elements of K in $D(x)$, we discover that

$$\begin{aligned} D(\alpha^5) &= (\alpha^5)^2 + \alpha^6\alpha^5 + \alpha^{14} = \alpha^{10} + \alpha^{11} + \alpha^{14} \\ &= (1+\alpha+\alpha^2) + (\alpha+\alpha^2+\alpha^3) + (1+\alpha^3) = 0; \\ D(\alpha^9) &= (\alpha^9)^2 + \alpha^6\alpha^9 + \alpha^{14} = \alpha^{18} + \alpha^{15} + \alpha^{14} = \alpha^3 + 1 + \alpha^{14} \\ &= \alpha^3 + 1 + (1+\alpha^3) = 0. \end{aligned}$$

Therefore α^5 and α^9 are the roots of $D(x)$, so errors occurred in the coefficients of x^5 and x^9. The received word

$$r(x) = x + x^7 + x^8 = 01000\underline{0}011\underline{0}00000$$

is corrected as

$$c(x) = x + x^5 + x^7 + x^8 + x^9 = 01000\underline{1}011\underline{1}00000,$$

which *is* a codeword (see page 461).

Similarly, if $r(x) = x^2 + x^6 + x^9 + x^{10} = 001000100110000$ is received, then

$$r(\alpha) = \alpha^8, \qquad r(\alpha^2) = \alpha, \qquad r(\alpha^3) = \alpha^9, \qquad \text{and}$$

$$\begin{aligned} D(x) &= x^2 + r(\alpha)x + \left[r(\alpha^2) + \frac{r(\alpha^3)}{r(\alpha)}\right] = x^2 + \alpha^8 x + \left(\alpha + \frac{\alpha^9}{\alpha^8}\right) \\ &= x^2 + \alpha^8 x + (\alpha + \alpha) = x^2 + \alpha^8 x = x(x + \alpha^8). \end{aligned}$$

The only nonzero root of $D(x)$ is α^8, so a single error occurred in the coefficient of x^8, and the correct word is

$$c(x) = x^2 + x^6 + x^8 + x^9 + x^{10} = 001000101110000.$$

Finally, if $1 + x + x^4$ is received, then

$$r(\alpha) = 1 + \alpha + \alpha^4 = 0 \qquad \text{and} \qquad r(\alpha^3) = 1 + \alpha^3 + \alpha^{12} = \alpha^5.$$

So $D(x)$ cannot be constructed, and we conclude that more than two errors have occurred. Similarly, if $1 + x + x^3$ is received, then verify that $D(x) = x^2 + \alpha^7 x + \alpha^5$ and that $D(x)$ has no roots in K. Once again, more than two errors have occurred.

EXERCISES

NOTE: *Unless stated otherwise, K is the field $\mathbf{Z}_2[x]/(1 + x + x^4)$ of order 16 and α is a root of $1 + x + x^4$, as in the example on pages 460–461.*

A. 1. (a) Prove that $f(x) + f(x) = 0$ for every $f(x) \in \mathbf{Z}_2[x]$.

(b) Prove that $u + u = 0$ for every u in the field K.

2. Show that the only irreducible quadratic in $\mathbf{Z}_2[x]$ is $x^2 + x + 1$. [*Hint:* List all the quadratics and use Corollary 4.14.]

3. Prove that $1 + x + x^4$ is irreducible in $\mathbf{Z}_2[x]$. [*Hint:* Exercise 2 and Corollary 4.14.]

4. Prove that the minimal polynomial of α^5 over $\mathbf{Z}_2$ is $1 + x + x^2$. [Use the table on page 460.]

5. (a) Prove that the minimal polynomial of α^3 over $\mathbf{Z}_2$ is $1 + x + x^2 + x^3 + x^4$. [*Hint:* Exercise 2, Corollary 4.14, and the table on page 460.]

   (b) Show that α^4 is also a root of $1 + x + x^4$.

B. 6. If $f(x) \in \mathbf{Z}_2[x]$ and α is an element in some extension field of $\mathbf{Z}_2$, prove that for every $k \geq 1$, $f(\alpha^{2k}) = f(\alpha^k)^2$. [*Hint:* Lemma 9.24.]

7. (a) Show that the function $f: \mathbf{Z}_2[x]/(x^n - 1) \to B(n)$ given by

$$f([a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}]) = (a_0, a_1, a_2, \ldots, a_{n-1})$$

   is surjective.

   (b) Prove that f is a homomorphism of additive groups.

   (c) Prove that f is injective [*Hint:* Theorem 7.27 in additive notation.]

8. (a) Let F be a field and $f(x) \in F[x]$. If $p(x)$ and $q(x)$ are distinct monic irreducibles in $F[x]$ such that $p(x) \mid f(x)$ and $q(x) \mid f(x)$, prove that $p(x)q(x) \mid f(x)$. [*Hint:* If $f(x) = q(x)h(x)$, then $p(x) \mid q(x)h(x)$; use part 2 of Theorem 4.8.]

   (b) If $m_1(x), m_2(x), \ldots, m_k(x)$ are distinct monic irreducibles in $F[x]$ such that each $m_i(x)$ divides $f(x)$, prove that $g(x) = m_1(x)m_2(x) \cdots m_k(x)$ divides $f(x)$.

9. Let C be the (15,7) BCH code of the examples in the text. Use the error-correction technique presented there to correct these received words or to determine that three or more errors have been made.

   (a) $1 + x = 110000000000000$.

   (b) $1 + x^3 + x^4 + x^5 = 100111000000000$.

   (c) $1 + x^2 + x^4 + x^7 = 101010010000000$.

   (d) $1 + x^6 + x^7 + x^8 + x^9 = 100000111100000$.

10. Show that the generator polynomial for the BCH code with $t = 3$, $r = 4$, $n = 15$ is $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. [Exercises 3–5 may be helpful.]

11. Let $K = \mathbf{Z}_2(\alpha)$ be a finite field of order 2^r, whose multiplicative group is generated by α. For each i, let $m_i(x)$ be the minimal polynomial of α^i over $\mathbf{Z}_2$. If $n = 2^r - 1$, prove that each $m_i(x)$ divides $x^n - 1$. [*Hint:* $\alpha^n = 1$ (why?); use Theorem 9.6.]

12. If $g(x)$ is the generator polynomial of a BCH code in $\mathbf{Z}_2[x]/(x^n - 1)$, prove that $g(x)$ divides $x^n - 1$. [*Hint:* Exercises 11 and 8(b).]

13. Let $g(x) \in \mathbf{Z}_2[x]$ be a divisor of $x^n - 1$ and let C be the principal ideal generated by $[g(x)]$ in $\mathbf{Z}_2[x]/(x^n - 1)$. Then C is a code. Prove that C is cyclic, meaning that C (with codewords written as elements of $B(n)$) has this property: If $(c_0, c_1, \ldots, c_{n-1}) \in C$, then $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. [*Hint:* $c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1} = x(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) - c_{n-1}(x^n - 1)$.]

C. 14. Let C be the code in Exercise 13. Assume $g(x)$ has degree m and let $k = n - m$. Let J be the set of all polynomials in $\mathbf{Z}_2[x]$ of the form $a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1}$.

(a) Prove that every element in C is of the form $[s(x)g(x)]$ with $s(x) \in J$. [*Hint:* Let $[h(x)g(x)] \in C$. By the Division Algorithm, $h(x)g(x) = e(x)(x^n - 1) + r(x)$, with $\deg r(x) < n$ and $[h(x)g(x)] = [r(x)]$. Show that $r(x) = s(x)g(x)$, where $s(x) = h(x) - e(x)f(x)$ and $g(x)f(x) = x^n - 1$. Use Theorem 4.1 to show $s(x) \in J$.]

(b) Prove that C has order 2^k and hence C is an (n,k) code. [*Hint:* Use Corollary 5.5 to show that if $s(x) \neq t(x)$ in J, then $[s(x)g(x)] \neq [t(x)g(x)]$ in C. How many elements are in J?]

15. Let C be the (15,7) BCH code of the examples in the text, with codewords written as polynomials of degree ≤ 14. Suppose the codeword $c(x)$ is transmitted with errors in the coefficients of x^i and x^j and $r(x)$ is received. Then $D(x) = (x + \alpha^i)(x + \alpha^j) \in K[x]$, whose roots are α^i and α^j, is the error-locator polynomial. Express the coefficients of $D(x)$ in terms of $r(\alpha)$, $r(\alpha^2)$, $r(\alpha^3)$ as follows.

(a) Show that $r(x) - c(x) = x^i + x^j$.

(b) Show that $r(\alpha^k) = \alpha^{ki} + \alpha^{kj}$ for $k = 1, 2, 3$. [See the boldface statement on page 462.]

(c) Show that $D(x) = x^2 + (\alpha^i + \alpha^j)x + \alpha^{i+j} = x^2 + r(\alpha)x + \alpha^{i+j}$.

(d) Show that $\alpha^{i+j} = r(\alpha^2) + \dfrac{r(\alpha^3)}{r(\alpha)}$. [*Hint:* Show that $r(\alpha)^3 = (\alpha^i + \alpha^j)^3 = \alpha^{3i} + \alpha^{3j} + \alpha^{i+j}(\alpha^i + \alpha^j) = r(\alpha^3) + r(\alpha)\alpha^{i+j}$ and solve for α^{i+j}; note that $r(\alpha)^2 = r(\alpha^2)$.]

16. Show that a BCH code with $t = 1$ is actually a Hamming code (see page 457).