7.7 CORRECTION OF ERRORS AND ERASURES

A q-ary t-error-correcting BCH (or RS) code can be used to correct all combinations of ν symbol errors and e symbol erasures provided that the inequality

$$\nu + e/2 \le t \tag{7.84}$$

holds. Each of the decoding algorithms presented in the last three sections can be modified to do the job.

Suppose the received polynomial $\mathbb{r}(X)$ contains ν symbol errors at positions $X^{i_1}, X^{i_2}, \cdots, X^{i_\nu}$, and e symbol erasures at positions $X^{j_1}, X^{j_2}, \cdots, X^{j_e}$. Because the erased positions are known, decoding is to find the locations and values of the errors and the values of the erased symbols. The erasure-location numbers corresponding to the erased positions $X^{j_1}, X^{j_2}, \cdots, X^{j_e}$ are $\alpha^{j_1}, \alpha^{j_2}, \cdots, \alpha^{j_e}$. We form the erasure-location polynomial:

$$\beta(X) \triangleq \prod_{l=1}^{e} (1 - \alpha^{j_l} X). \tag{7.85}$$

Now, we fill the e erased positions in $\mathbb{r}(X)$ with zeros (or arbitrary symbols from $GF(q)$). This substitution of e zeros into the erased positions in $\mathbb{r}(X)$ can introduce up to e additional errors. Let $\mathbb{r}^*(X)$ denote the modified received polynomial. Let

$$\sigma(X) \triangleq \prod_{k=1}^{\nu} (1 - \alpha^{i_k} X) \tag{7.86}$$

be the error-location polynomial for the errors in $\mathbb{r}(X)$ at positions $X^{i_1}, X^{i_2}, \cdots, X^{i_\nu}$. Then, the error-location polynomial for the modified received polynomial $\mathbb{r}^*(X)$ is

$$\gamma(X) = \sigma(X)\beta(X), \tag{7.87}$$

for which $\beta(X)$ is known. Now, decoding is to find $\sigma(X)$ and the error-value evaluator $\mathbb{Z}_0(X)$ for $\mathbb{r}^*(X)$.

We compute the syndrome polynomial

$$\mathbb{S}(X) = S_1 + S_2 X + \cdots + S_{2t} X^{2t-1}$$

from the modified received polynomial $\mathbb{r}^*(X)$. Then, the key equation becomes

$$\sigma(X)\beta(X)\mathbb{S}(X) \equiv \mathbb{Z}_0(X) \bmod X^{2t}. \tag{7.88}$$

The decoding problem is to find the solution $(\sigma(X), \mathbb{Z}_0(X))$ of this equation such that $\sigma(X)$ has minimum degree ν, and $\deg \mathbb{Z}_0(X) < \nu + e$. Since $\beta(X)$ and $\mathbb{S}(X)$ are known, we can combine them. Let

$$\begin{aligned} \mathbb{T}(X) &\triangleq [\beta(X)\mathbb{S}(X)]_{2t} \\ &= T_1 + T_2 X + \cdots + T_{2t} X^{2t-1} \end{aligned} \tag{7.89}$$

denote the polynomial that consists of the $2t$ terms of $\beta(X)\mathbb{S}(X)$ from X^0 to X^{2t-1}. Then, we can write the key equation of (7.88) as

$$\sigma(X)\mathbb{T}(X) \equiv \mathbb{Z}_0(X) \bmod X^{2t}. \tag{7.90}$$

This key equation may be solved by using either Euclid's or Berlekamp's algorithm.

The Euclidean algorithm for error/erasure decoding consists of the following:

1. Compute the erasure-location polynomial $\beta(X)$ using the erasure information from the received polynomial $\mathbb{r}(X)$.
2. Form the modified received polynomial $\mathbb{r}^*(X)$ by replacing the erased symbols with zeros. Compute the syndrome polynomial $\mathbb{S}(X)$ from $\mathbb{r}^*(X)$.
3. Compute the modified syndrome polynomial $\mathbb{T}(X) = [\beta(X)\,\mathbb{S}(X)]_{2t}$.
4. Set the following initial conditions:

$$\mathbb{Z}_0^{(-1)}(X) = X^{2t}, \quad \mathbb{Z}_0^{(0)}(X) = \mathbb{T}(X),$$
$$\sigma^{(-1)}(X) = 0, \quad \text{and} \quad \sigma^{(0)}(X) = 1.$$

5. Execute the Euclidean algorithm iteratively as described in Section 7.5 until a step ρ is reached for which

$$\deg \mathbb{Z}_0^{(\rho)}(X) < \begin{cases} t + e/2, & \text{for even } e, \\ t + (e-1)/2, & \text{for odd } e. \end{cases} \tag{7.91}$$

Then, set $\sigma(X) = \sigma^{(\rho)}(X)$, and $\mathbb{Z}_0(X) = \mathbb{Z}_0^{(\rho)}(X)$.

6. Find the roots of $\sigma(X)$ and determine the error locations in $\mathbb{r}(X)$.
7. Determine the values of errors and erasures from $\mathbb{Z}_0(X)$ and $\gamma(X) = \sigma(X)\beta(X)$. The error values are given by

$$e_{i_k} = \frac{-\mathbb{Z}_0(\alpha^{-i_k})}{\gamma'(\alpha^{-i_k})} \tag{7.92}$$

for $1 \le k \le \nu$, and the values of the erased symbols are given by

$$f_{j_l} = \frac{-\mathbb{Z}_0(\alpha^{-j_l})}{\gamma'(\alpha^{-j_l})} \tag{7.93}$$

for $1 \le l \le e$, where $\gamma'(X)$ is the derivative of the overall error/erasure-location polynomial $\gamma(X) = \sigma(X)\beta(X)$; that is,

$$\gamma'(X) = \frac{d}{dX}\gamma(X)$$
$$= -a \sum_{l=1}^{\nu+e} \alpha^{j_l} \prod_{i=1, i\neq l}^{\nu+e} (1 - \alpha^{j_i} X). \tag{7.94}$$

(a is the constant $\neq 1$ that may appear in $\sigma(X)$ when the Euclidean algorithm is used).

EXAMPLE 7.8

Again consider the triple-error-correcting RS code of length 15 over $GF(2^4)$ generated by $g(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)$. This code is capable of correcting all combinations of two or fewer errors and two or fewer erasures. Suppose the all-zero codeword is transmitted, and the received vector is

$$r = (000 * 00 * 00\alpha 00\alpha^4 00),$$

where $*$ denotes an erasure. The received polynomial is

$$r(X) = (*)X^3 + (*)X^6 + \alpha X^9 + \alpha^4 X^{12}.$$

Because the erased positions are X^3 and X^6, the erasure-location polynomial is

$$\begin{aligned}\beta(X) &= (1+\alpha^3 X)(1+\alpha^6 X)\\ &= 1 + \alpha^2 X + \alpha^9 X^2.\end{aligned}$$

Replacing the erased symbols with zeros, we obtain the following modified received polynomial:

$$r^*(X) = \alpha X^9 + \alpha^4 X^{12}.$$

The syndrome components computed from $r^*(X)$ are

$$\begin{aligned} S_1 &= r^*(\alpha) = \alpha^8, & S_4 &= r^*(\alpha^4) = 0,\\ S_2 &= r^*(\alpha^2) = \alpha^{11}, & S_5 &= r^*(\alpha^5) = 1,\\ S_3 &= r^*(\alpha^3) = \alpha^9, & S_6 &= r^*(\alpha^6) = \alpha^8.\end{aligned}$$

The syndrome polynomial is then

$$S(X) = \alpha^8 + \alpha^{11}X + \alpha^9 X^2 + X^4 + \alpha^8 X^5,$$

and the modified syndrome polynomial is

$$\begin{aligned}T(X) &= [\beta(X)S(X)]_{2t}\\ &= \alpha^8 + \alpha^{14}X + \alpha^4 X^2 + \alpha^3 X^3 + \alpha^{14} X^4 + X^5.\end{aligned}$$

Using the Euclidean decoding algorithm, we set the initial conditions as follows:

$$\begin{aligned} Z_0^{(-1)}(X) &= X^6, \quad Z_0^{(0)}(X) = T(X),\\ \sigma^{(-1)}(X) &= 0, \quad \text{and} \quad \sigma^{(0)}(X) = 1.\end{aligned}$$

Since $t = 3$ and $e = 2$, the algorithm terminates when $\deg Z_0(X) < 4$. Executing the algorithm, we obtain Table 7.6. The error-location polynomial is

$$\begin{aligned}\sigma(X) &= \alpha(1 + \alpha^8 X + \alpha^6 X^2)\\ &= \alpha(1+\alpha^9 X)(1+\alpha^{12}X).\end{aligned}$$

The two roots of $\sigma(X)$ are α^{-9} and α^{-12}. The reciprocals of these two roots give the error locations, α^9 and α^{12}. The error-value evaluator is

$$\mathbf{Z}_0(X) = \alpha^9 + \alpha^8 X + \alpha X^2 + \alpha X^3.$$

The overall error/erasure-location polynomial is

$$\begin{aligned}\gamma(X) &= \sigma(X)\beta(X) \\ &= \alpha(1+\alpha^3 X)(1+\alpha^6 X)(1+\alpha^9 X)(1+\alpha^{12} X),\end{aligned}$$

and its derivative is

$$\begin{aligned}\gamma'(X) = {} & \alpha^4(1+\alpha^6 X)(1+\alpha^9 X)(1+\alpha^{12} X) \\ & + \alpha^7(1+\alpha^3 X)(1+\alpha^9 X)(1+\alpha^{12} X) \\ & + \alpha^{10}(1+\alpha^3 X)(1+\alpha^6 X)(1+\alpha^{12} X) \\ & + \alpha^{13}(1+\alpha^3 X)(1+\alpha^6 X)(1+\alpha^9 X).\end{aligned}$$

It follows from (7.92) and (7.93) that the error values at positions X^9 and X^{12} are

$$e_9 = \frac{-\mathbf{Z}_0(\alpha^{-9})}{\gamma'(\alpha^{-9})} = \frac{\alpha^{13}}{\alpha^{12}} = \alpha,$$

$$e_{12} = \frac{-\mathbf{Z}_0(\alpha^{-12})}{\gamma'(\alpha^{-12})} = \frac{\alpha^3}{\alpha^{14}} = \alpha^{-11} = \alpha^4,$$

and the values of the erased symbols at positions X^3 and X^6 are

$$f_3 = \frac{-\mathbf{Z}_0(\alpha^{-3})}{\gamma'(\alpha^{-3})} = \frac{0}{\alpha^8} = 0,$$

$$f_6 = \frac{-\mathbf{Z}_0(\alpha^{-6})}{\gamma'(\alpha^{-6})} = \frac{0}{1} = 0.$$

Then, the estimated error polynomial is

$$\mathbf{e}(X) = \alpha X^9 + \alpha^4 X^{12}.$$

Subtracting $\mathbf{e}(X)$ from $\mathbf{r}^*(X)$, we obtain the decoded code polynomial $\mathbf{v}(X) = \mathbf{0}$, which is the transmitted code polynomial.

EXAMPLE 7.9

Consider the (63, 55, 9) RS code generated by

$$\begin{aligned}g(X) &= (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)(X+\alpha^7)(X+\alpha^8) \\ &= X^8 + \alpha^{43}X^7 + \alpha^{59}X^6 + \alpha^{31}X^5 + \alpha^{10}X^4 + \alpha^{40}X^3 + \alpha^{14}X^2 + \alpha^7 X + \alpha^{36}.\end{aligned}$$

TABLE 7.6: Steps for finding the error-location polynomial and error-value evaluator of the RS code given in Example 7.6.

i	$\mathbb{Z}_{\mathbb{0}}^{(i)}(X)$	$\mathbb{q}_i(X)$	$\sigma^{(i)}(X)$
-1	X^6	—	0
0	$\mathbb{T}(X)$	—	1
1	$\alpha^7 + \alpha^3 X + X^2 + \alpha^{10} X^3 + \alpha^8 X^4$	$\alpha^{14} + X$	$\alpha^{14} + X$
2	$\alpha^9 + \alpha^8 X + \alpha X^2 + \alpha X^3$	$\alpha^5 + \alpha^7 X$	$\alpha + \alpha^9 X + \alpha^7 X^2$

This code is capable of correcting all combinations of three or fewer errors and two or fewer erasures. Suppose the all-zero codeword is transmitted, and the received vector is

$$\mathbb{r} = (000000\alpha^{15}0000000000000\alpha^{37}0000000 * 000$$
$$00\alpha^{4}00000000000000000 * 000000000).$$

The received polynomial is

$$\mathbb{r} = \alpha^{15}X^6 + \alpha^{37}X^{20} + (*)X^{28} + \alpha^4 X^{34} + (*)X^{53}.$$

Because the erased positions are X^{28} and X^{53}, the erasure-location polynomial is

$$\beta(X) = (1 + \alpha^{28}X)(1 + \alpha^{53}X)$$
$$= 1 + \alpha^{39}X + \alpha^{18}X^2.$$

Replacing the erased symbols with zeros, we obtain the following modified received polynomial:

$$\mathbb{r}^*(X) = \alpha^{15}X^6 + \alpha^{37}X^{20} + \alpha^4 X^{34}.$$

The syndrome components computed from $\mathbb{r}^*(X)$ are

$$\begin{aligned} S_1 &= \mathbb{r}^*(\alpha) = \alpha^{19}, & S_5 &= \mathbb{r}^*(\alpha^5) = \alpha^{43}, \\ S_2 &= \mathbb{r}^*(\alpha^2) = \alpha, & S_6 &= \mathbb{r}^*(\alpha^6) = \alpha^4, \\ S_3 &= \mathbb{r}^*(\alpha^3) = 1, & S_7 &= \mathbb{r}^*(\alpha^7) = \alpha^{58}, \\ S_4 &= \mathbb{r}^*(\alpha^4) = \alpha^{22}, & S_8 &= \mathbb{r}^*(\alpha^8) = \alpha^{28}. \end{aligned}$$

The syndrome polynomial is then

$$\mathbb{S}(X) = \alpha^{19} + \alpha X + X^2 + \alpha^{22}X^3 + \alpha^{43}X^4 + \alpha^4 X^5 + \alpha^{58}X^6 + \alpha^{28}X^7,$$

and the modified syndrome polynomial is

$$\mathbb{T}(X) = [\beta(X)\mathbb{S}(X)]_{2t}$$
$$= \alpha^{19} + \alpha^{59}X + \alpha X^2 + \alpha^{41}X^3 + \alpha^{32}X^4 + \alpha^{62}X^5 + \alpha^{60}X^6 + \alpha^{48}X^7.$$

Using the Euclidean decoding algorithm, we set the initial condition as follows:

$$\mathbb{Z}_0^{(-1)}(X) = X^8, \quad \mathbb{Z}_0^{(0)}(X) = \mathbb{T}(X),$$
$$\sigma^{(-1)}(X) = 0, \quad \text{and} \quad \sigma^{(0)}(X) = 1.$$

TABLE 7.7: Steps finding the error-location polynomial and error-value evaluator of the (63,55,9) RS code over $GF(2^6)$ given in Example 7.9.

i	$\mathbf{Z}_0^{(i)}(X)$	$q_i(X)$	$\sigma(X)$
-1	X^8	—	0
0	$\mathbf{T}(X)$	—	1
1	$\alpha^{46}+\alpha^{48}X+\alpha^{58}X^2+\alpha^{30}X^3$ $+\alpha^{25}X^4+\alpha^{5}X^5+\alpha^{12}X^6$	$\alpha^{27}+\alpha^{15}X$	$\alpha^{27}+\alpha^{15}X$
2	$\alpha^{57}+\alpha^{31}X+\alpha^{56}X^2+\alpha^{44}X^3$ $+\alpha^{17}X^4+\alpha^{19}X^5$	$\alpha^{22}+\alpha^{36}X$	$\alpha^{38}+\alpha^{44}X+\alpha^{51}X^2$
3	$\alpha^{3}+\alpha^{53}X+\alpha^{30}X^2$ $+\alpha^{24}X^3+\alpha^{13}X^4$	$\alpha^{48}+\alpha^{56}X$	$\alpha^{47}+\alpha^{22}X+\alpha^{42}X^2+\alpha^{44}X^3$

Since $t = 4$ and $e = 2$, the algorithm terminates when $\deg \mathbf{Z}_0(X) < 5$. Executing the algorithm, we obtain Table 7.7. The error-location polynomial is

$$\begin{aligned}\sigma(X) &= \alpha^{47}(1+\alpha^{38}X+\alpha^{58}X^2+\alpha^{60}X^3)\\ &= \alpha^{47}(1+\alpha^{6}X)(1+\alpha^{20}X)(1+\alpha^{34}X).\end{aligned}$$

The three roots of $\sigma(X)$ are α^{-6}, α^{-20}, and α^{-34}. The reciprocals of these three roots give the error locations, α^6, α^{20}, and α^{34}. The error-value evaluator is

$$\mathbf{Z}_0(X) = \alpha^3+\alpha^{53}X+\alpha^{30}X^2+\alpha^{24}X^3+\alpha^{13}X^4.$$

The overall error/erasure-location polynomial is

$$\begin{aligned}\gamma(X) &= \sigma(X)\beta(X)\\ &= \alpha^{47}(1+\alpha^{6}X)(1+\alpha^{20}X)(1+\alpha^{28}X)(1+\alpha^{34}X)(1+\alpha^{53}X)\\ &= \alpha^{47}+\alpha^{28}X+\alpha^{18}X^2+\alpha^{48}X^3+\alpha^{12}X^4+\alpha^{62}X^5,\end{aligned}$$

and its derivative is

$$\gamma'(X) = \alpha^{28}+\alpha^{48}X^2+\alpha^{62}X^4.$$

The error values at positions X^6, X^{20}, and X^{34} are

$$e_6 = \frac{-\mathbf{Z}_0(\alpha^{-6})}{\gamma'(\alpha^{-6})} = \frac{\alpha^{39}}{\alpha^{24}} = \alpha^{15},$$

$$e_{20} = \frac{-\mathbf{Z}_0(\alpha^{-20})}{\gamma'(\alpha^{-20})} = \frac{\alpha^{6}}{\alpha^{32}} = \alpha^{37},$$

$$e_{34} = \frac{-\mathbf{Z}_0(\alpha^{-34})}{\gamma'(\alpha^{-34})} = \frac{\alpha^{61}}{\alpha^{57}} = \alpha^{4},$$

and the values of the erased symbols at positions X^{28} and X^{53} are

$$f_{28} = \frac{-\mathbb{Z}_0(\alpha^{-28})}{\gamma'(\alpha^{-28})} = \frac{0}{\alpha^{29}} = 0,$$

$$f_{53} = \frac{-\mathbb{Z}_0(\alpha^{-53})}{\gamma'(\alpha^{-53})} = \frac{0}{\alpha^{13}} = 0.$$

Then, the estimated error polynomial is

$$\mathbb{e}(X) = \alpha^{15}X^6 + \alpha^{37}X^{20} + \alpha^4 X^{34}.$$

Subtracting $\mathbb{e}(X)$ from $\mathbb{r}^*(X)$, we obtain the decoded code polynomial $\mathbb{v}(X) = \mathbb{0}$, which is the transmitted code polynomial.

PROBLEMS

7.1 Consider the triple-error-correcting RS code given in Example 7.2. Find the code polynomial for the message

$$\mathbb{a}(X) = 1 + \alpha^5 X + \alpha X^4 + \alpha^7 X^8.$$

7.2 Using the Galois field $GF(2^5)$ given in Appendix A, find the generator polynomials of the double-error-correcting and triple-error-correcting RS codes of length 31.

7.3 Using the Galois field $GF(2^6)$ given in Table 6.2, find the generator polynomials of double-error-correcting and triple-error-correcting RS codes of length 63.

7.4 Consider the triple-error-correcting RS code of length 15 given in Example 7.2. Decode the received polynomial

$$\mathbb{r}(X) = \alpha^4 X^3 + \alpha^9 X^8 + \alpha^3 X^{13}$$

using the Berlekamp algorithm.

7.5 Continue Problem 7.4. Decode the received polynomial with the Euclidean algorithm.

7.6 Consider the triple-error-correcting RS code of length 31 constructed in Problem 7.2. Decode the received polynomial

$$\mathbb{r}(X) = \alpha^2 + \alpha^{21}X^{12} + \alpha^7 X^{20}$$

using the Euclidean algorithm.

7.7 Continue Problem 7.6. Decode the received polynomial in the frequency domain using transform decoding.

7.8 For the same RS code of Problem 7.6, decode the following received polynomial with two erasures:

$$\mathbb{r}(X) = (*)X^3 + \alpha^5 X^7 + (*)X^{18} + \alpha^3 X^{21}$$

with the Euclidean algorithm.

7.9 Prove that the dual code of a RS code is also a RS code.

7.10 Prove that the $(2^m - 1, k)$ RS code with minimum distance d contains the primitive binary BCH code of length $2^m - 1$ with designed distance d as a subcode. This subcode is called a *subfield subcode.*