Chapter 7

7.2 The generator polynomial of the double-error-correcting RS code over GF(2^5) is

$$\begin{aligned}\mathbf{g}(X) &= (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4) \\ &= \alpha^{10}+\alpha^{29}X+\alpha^{19}X^2+\alpha^{24}X^3+X^4.\end{aligned}$$

The generator polynomial of the triple-error-correcting RS code over GF(2^5) is

$$\begin{aligned}\mathbf{g}(X) &= (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6) \\ &= \alpha^{21}+\alpha^{24}X+\alpha^{16}X^2+\alpha^{24}X^3+\alpha^{9}X^4+\alpha^{10}X^5+X^6.\end{aligned}$$

7.4 The syndrome components of the received polynomial are:

$$S_1 = \boldsymbol{r}(\alpha) = \alpha^7+\alpha^2+\alpha = \alpha^{13},$$
$$S_2 = \boldsymbol{r}(\alpha^2) = \alpha^{10}+\alpha^{10}+\alpha^{14} = \alpha^{14},$$
$$S_3 = \boldsymbol{r}(\alpha^3) = \alpha^{13}+\alpha^{3}+\alpha^{12} = \alpha^{9},$$
$$S_4 = \boldsymbol{r}(\alpha^4) = \alpha+\alpha^{11}+\alpha^{10} = \alpha^{7},$$
$$S_5 = \boldsymbol{r}(\alpha^5) = \alpha^4+\alpha^{4}+\alpha^{8} = \alpha^{8},$$
$$S_6 = \boldsymbol{r}(\alpha^6) = \alpha^7+\alpha^{12}+\alpha^{6} = \alpha^{3}.$$

The iterative procedure for finding the error location polynomial is shown in Table P.7.4. The error location polynomial is

$$\boldsymbol{\sigma}(X) = 1+\alpha^9X^3.$$

The roots of this polynomial are α^2, α^7, and α^{12}. Hence the error location numbers are α^3, α^8, and α^{13}.

From the syndrome components of the received polynomial and the coefficients of the error

Table P.7.4

μ	$\boldsymbol{\sigma}^{\mu}(X)$	d_μ	l_μ	$\mu - l_\mu$
-1	1	1	0	-1
0	1	α^{13}	0	0
1	$1+\alpha^{13}X$	α^{10}	1	0 (take $\rho = -1$)
2	$1+\alpha X$	α^{7}	1	1 (take $\rho = 0$)
3	$1+\alpha^{13}X+\alpha^{10}X^2$	α^{9}	2	1 (take $\rho = 1$)
4	$1+\alpha^{14}X+\alpha^{12}X^2$	α^{8}	2	2 (take $\rho = 2$)
5	$1+\alpha^{9}X^3$	0	3	2 (take $\rho = 3$)
6	$1+\alpha^{9}X^3$	$-$	$-$	$-$

location polynomial, we find the error value evaluator,

$$\begin{aligned}
\mathbf{Z}_0(X) &= S_1 + (S_2 + \sigma_1 S_1)X + (S_3 + \sigma_1 S_2 + \sigma_2 S_1)X^2 \\
&= \alpha^{13} + (\alpha^{14} + 0\alpha^{13})X + (\alpha^{9} + 0\alpha^{14} + 0\alpha^{13})X^2 \\
&= \alpha^{13} + \alpha^{14}X + \alpha^{9}X^2.
\end{aligned}$$

The error values at the positions X^3, X^8, and X^{13} are:

$$e_3 = \frac{-\mathbf{Z}_0(\alpha^{-3})}{\boldsymbol{\sigma}'(\alpha^{-3})} = \frac{\alpha^{13}+\alpha^{11}+\alpha^{3}}{\alpha^{3}(1+\alpha^{8}\alpha^{-3})(1+\alpha^{13}\alpha^{-3})} = \frac{\alpha^7}{\alpha^3} = \alpha^4,$$

$$e_8 = \frac{-\mathbf{Z}_0(\alpha^{-8})}{\boldsymbol{\sigma}'(\alpha^{-8})} = \frac{\alpha^{13}+\alpha^{6}+\alpha^{8}}{\alpha^{8}(1+\alpha^{3}\alpha^{-8})(1+\alpha^{13}\alpha^{-8})} = \frac{\alpha^2}{\alpha^8} = \alpha^9,$$

$$e_{13} = \frac{-\mathbf{Z}_0(\alpha^{-13})}{\boldsymbol{\sigma}'(\alpha^{-13})} = \frac{\alpha^{13}+\alpha+\alpha^{13}}{\alpha^{13}(1+\alpha^{3}\alpha^{-13})(1+\alpha^{8}\alpha^{-13})} = \frac{\alpha}{\alpha^{13}} = \alpha^3.$$

Consequently, the error pattern is

$$\boldsymbol{e}(X) = \alpha^4 X^3 + \alpha^9 X^8 + \alpha^3 X^{13}.$$

and the decoded codeword is the all-zero codeword.

7.5 The syndrome polynomial is

$$\mathbf{S}(X) = \alpha^{13} + \alpha^{14}X + \alpha^{9}X^2 + \alpha^{7}X^3 + \alpha^{8}X^4 + \alpha^{3}X^5$$

Table P.7.5 displays the steps of Euclidean algorithm for finding the error location and error value polynomials.

Table P.7.5

i	$\mathbf{Z}_0^{(i)}(X)$	$\boldsymbol{q}_i(X)$	$\boldsymbol{\sigma}_i(X)$
-1	X^6	$-$	0
0	$\alpha^{13} + \alpha^{14}X + \alpha^{9}X^2 + \alpha^{7}X^3 + \alpha^{8}X^4 + \alpha^{3}X^5$	$-$	1
1	$1 + \alpha^{8}X + \alpha^{5}X^3 + \alpha^{2}X^4$	$\alpha^2 + \alpha^{12}X$	$\alpha^2 + \alpha^{12}X$
2	$\alpha + \alpha^{13}X + \alpha^{12}X^3$	$\alpha^{12} + \alpha X$	$\alpha^3 + \alpha X + \alpha^{13}X^2$
3	$\alpha^7 + \alpha^8 X + \alpha^3 X^2$	$\alpha^8 + \alpha^5 X$	$\alpha^9 + \alpha^3 X^3$

The error location and error value polynomials are:

$$\boldsymbol{\sigma}(X) = \alpha^9 + \alpha^3X^3 = \alpha^9(1 + \alpha^9X^3)$$

$$\mathbf{Z}_0(X) = \alpha^7 + \alpha^8X + \alpha^3X^2 = \alpha^9(\alpha^{13} + \alpha^{14}X + \alpha^9X^2)$$

From these polynomials, we find that the error location numbers are α^3, α^8, and α^{13}, and error values are

$$e_3 = \frac{-\mathbf{Z}_0(\alpha^{-3})}{\boldsymbol{\sigma}'(\alpha^{-3})} = \frac{\alpha^7 + \alpha^5 + \alpha^{12}}{\alpha^9\alpha^3(1 + \alpha^8\alpha^{-3})(1 + \alpha^{13}\alpha^{-3})} = \frac{\alpha}{\alpha^{12}} = \alpha^4,$$

$$e_8 = \frac{-\mathbf{Z}_0(\alpha^{-8})}{\boldsymbol{\sigma}'(\alpha^{-8})} = \frac{\alpha^7 + 1 + \alpha^2}{\alpha^9\alpha^8(1 + \alpha^3\alpha^{-8})(1 + \alpha^{13}\alpha^{-8})} = \frac{\alpha^{11}}{\alpha^2} = \alpha^9,$$

$$e_{13} = \frac{-\mathbf{Z}_0(\alpha^{-13})}{\boldsymbol{\sigma}'(\alpha^{-13})} = \frac{\alpha^7 + \alpha^{10} + \alpha^7}{\alpha^9\alpha^{13}(1 + \alpha^3\alpha^{-13})(1 + \alpha^8\alpha^{-13})} = \frac{\alpha^{10}}{\alpha^7} = \alpha^3.$$

Hence the error pattern is

$$\boldsymbol{e}(X) = \alpha^4 X^3 + \alpha^9 X^8 + \alpha^3 X^{13}.$$

and the received polynomial is decoded into the all-zero codeword.

7.6 From the received polynomial,

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

we compute the syndrome,

$$\begin{aligned}
S_1 &= \mathbf{r}(\alpha^1) = \alpha^2 + \alpha^{33} + \alpha^{27} = \alpha^{27}, \\
S_2 &= \mathbf{r}(\alpha^2) = \alpha^2 + \alpha^{45} + \alpha^{47} = \alpha, \\
S_3 &= \mathbf{r}(\alpha^3) = \alpha^2 + \alpha^{57} + \alpha^{67} = \alpha^{28}, \\
S_4 &= \mathbf{r}(\alpha^4) = \alpha^2 + \alpha^{69} + \alpha^{87} = \alpha^{29}, \\
S_5 &= \mathbf{r}(\alpha^5) = \alpha^2 + \alpha^{81} + \alpha^{107} = \alpha^{15}, \\
S_6 &= \mathbf{r}(\alpha^6) = \alpha^2 + \alpha^{93} + \alpha^{127} = \alpha^8.
\end{aligned}$$

Therefore, the syndrome polynomial is

$$\mathbf{S}(X) = \alpha^{27} + \alpha X + \alpha^{28} X^2 + \alpha^{29} X^3 + \alpha^{15} X^4 + \alpha^8 X^5$$

Using the Euclidean algorithm, we find

$$\begin{aligned}
\boldsymbol{\sigma}(X) &= \alpha^{23} X^3 + \alpha^9 X + \alpha^{22}, \\
\mathbf{Z}_0(X) &= \alpha^{26} X^2 + \alpha^6 X + \alpha^{18},
\end{aligned}$$

as shown in the following table: The roots of $\boldsymbol{\sigma}(X)$ are: $1 = \alpha^0$, α^{11} and α^{19}. From these roots, we find the error location numbers: $\beta_1 = (\alpha^0)^{-1} = \alpha^0$, $\beta_2 = (\alpha^{11})^{-1} = \alpha^{20}$, and

i	$\mathbf{Z}_0^{(i)}(X)$	$\mathbf{q}_i(X)$	$\boldsymbol{\sigma}_i(X)$
-1	X^6	-	0
0	**S**(X)	-	1
1	$\alpha^5X^4+\alpha^9X^3+\alpha^{22}X^2+\alpha^{11}X+\alpha^{26}$	$\alpha^{23}X+\alpha^{30}$	$\alpha^{23}X+\alpha^{30}$
2	$\alpha^8X^3+\alpha^4X+\alpha^6$	$\alpha^3X+\alpha^5$	$\alpha^{24}X^2+\alpha^{30}X+\alpha^{10}$
3	$\alpha^{26}X^2+\alpha^6X+\alpha^{18}$	$\alpha^{28}X+\alpha$	$\alpha^{23}X^3+\alpha^9X+\alpha^{22}$

$\beta^3=(\alpha^{19})^{-1}=\alpha^{12}$. Hence the error pattern is

$$\mathbf{e}(X)=e_0+e_{12}X^{12}+e_{20}X^{20}.$$

The error location polynomial and its derivative are:

$$\begin{aligned}\boldsymbol{\sigma}(X) &= \alpha^{22}(1+X)(1+\alpha^{12}X)(1+\alpha^{20}X),\\ \boldsymbol{\sigma}'(X) &= \alpha^{22}(1+\alpha^{12}X)(1+\alpha^{20}X)+\alpha^3(1+X)(1+\alpha^{20}X)+\alpha^{11}(1+X)(1+\alpha^{12}X).\end{aligned}$$

The error values at the 3 error locations are given by:

$$\begin{aligned}e_0 &= \frac{-\mathbf{Z}_0(\alpha^0)}{\boldsymbol{\sigma}'(\alpha^0)}=\frac{\alpha^{26}+\alpha^6+\alpha^8}{\alpha^{22}(1+\alpha^{12})(1+\alpha^{20})}=\alpha^2,\\ e_{12} &= \frac{-\mathbf{Z}_0(\alpha^{-12})}{\boldsymbol{\sigma}'(\alpha^{-12})}=\frac{\alpha^2+\alpha^{25}+\alpha^{18}}{\alpha^3(1+\alpha^{19})(1+\alpha^8)}=\alpha^{21},\\ e_{20} &= \frac{-\mathbf{Z}_0(\alpha^{-20})}{\boldsymbol{\sigma}'(\alpha^{-20})}=\frac{\alpha^{17}+\alpha^{17}+\alpha^{18}}{\alpha^{11}(1+\alpha^{11})(1+\alpha^{23})}=\alpha^7.\end{aligned}$$

Hence, the error pattern is

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

and the decoded codeword is

$$\mathbf{v}(X)=\mathbf{r}(X)-\mathbf{e}(X)=\mathbf{0}.$$

7.9 Let **g**(X) be the generator polynomial of a t-symbol correcting RS code $\mathcal{C}$ over GF(q) with α, $\alpha^2, \ldots, \alpha^{2t}$ as roots, where α is a primitive element of GF(q). Since $\mathbf{g}(X)$ divides $X^{q-1}-1$, then

$$X^{q-1} - 1 = \mathbf{g}(X)\mathbf{h}(X).$$

The polynomial $\mathbf{h}(X)$ has $\alpha^{2t+1}, \ldots, \alpha^{q-1}$ as roots and is called the parity polynomial. The dual code $\mathcal{C}_d$ of $\mathcal{C}$ is generated by the reciprocal of $\mathbf{h}(X)$,

$$\mathbf{h}^*(X) = X^{q-1-2t}\mathbf{h}(X^{-1}).$$

We see that $\mathbf{h}^*(X)$ has $\alpha^{-(2t+1)} = \alpha^{q-2t-2}$, $\alpha^{-(2t+2)} = \alpha^{q-2t-3}$, $\ldots$, $\alpha^{-(q-2)} = \alpha$, and $\alpha^{-(q-1)} = 1$ as roots. Thus $\mathbf{h}^*(X)$ has the following consecutive powers of α as roots:

$$1, \alpha, \alpha^2, \ldots, \alpha^{q-2t-2}.$$

Hence $\mathcal{C}_d$ is a $(q-1, 2t, q-2t)$ RS code with minimum distance $q-2t$.

7.10 The generator polynomial $\mathbf{g}_{rs}(X)$ of the RS code $\mathcal{C}$ has $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ as roots. Note that GF(2^m) has GF(2) as a subfield. Consider those polynomial $\mathbf{v}(X)$ over GF(2) with degree 2^m-2 or less that has $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ (also their conjugates) as roots. These polynomials over GF(2) form a primitive BCH code $\mathcal{C}_{bch}$ with designed distance d. Since these polynomials are also code polynomials in the RS code $\mathcal{C}_{rs}$, hence $\mathcal{C}_{bch}$ is a subcode of $\mathcal{C}_{rs}$.

7.11 Suppose $\mathbf{c}(X) = \sum_{i=0}^{2^m-2} c_i X^i$ is a minimum weight code polynomial in the $(2^m-1, k)$ RS code $\mathcal{C}$. The minimum weight is increased to $d+1$ provided

$$c_\infty = -\mathbf{c}(1) = -\sum_{i=0}^{2^m-2} c_i \neq 0.$$

We know that $\mathbf{c}(X)$ is divisible by $\mathbf{g}(X)$. Thus $\mathbf{c}(X) = \mathbf{a}(X)\mathbf{g}(X)$ with $\mathbf{a}(X) \neq 0$. Consider

$$\mathbf{c}(1) = \mathbf{a}(1)\mathbf{g}(1).$$

Since 1 is not a root of $\mathbf{g}(X)$, $\mathbf{g}(1) \neq 0$. If $\mathbf{a}(1) \neq 0$, then $c_\infty = -\mathbf{c}(1) \neq 0$ and the vector $(c_\infty, c_0, c_1, \ldots, c_{2^m-2})$ has weight $d+1$. Next we show that $\mathbf{a}(1)$ is not equal to 0. If $\mathbf{a}(1) = 0$, then $\mathbf{a}(X)$ has $X - 1$ as a factor and $\mathbf{c}(X)$ is a multiple of $(X-1)\mathbf{g}(X)$ and must have a weight at least $d+1$. This contradicts to the hypothesis that $\mathbf{c}(X)$ is a minimum weight code polynomial. Consequently the extended RS code has a minimum distance $d+1$.

7.12 To prove the minimum distance of the doubly extended RS code, we need to show that no $2t$ or fewer columns of $\mathbf{H}_1$ sum to zero over GF(2^m) and there are $2t+1$ columns in $\mathbf{H}_1$ sum to zero. Suppose there are δ columns in $\mathbf{H}_1$ sum to zero and $\delta \leq 2t$. There are 4 case to be considered:

(1) All δ columns are from the same submatrix $\mathbf{H}$.

(2) The δ columns consist of the first column of $\mathbf{H}_1$ and $\delta - 1$ columns from $\mathbf{H}$.

(3) The δ columns consist of the second column of $\mathbf{H}_1$ and $\delta - 1$ columns from $\mathbf{H}$.

(4) The δ columns consist of the first two columns of $\mathbf{H}_1$ and $\delta - 2$ columns from $\mathbf{H}$.

The first case leads to a $\delta \times \delta$ Vandermonde determinant. The second and third cases lead to a $(\delta-1)\times(\delta-1)$ Vandermonde determinant. The 4th case leads to a $(\delta-2)\times(\delta-2)$ Vandermonde determinant. The derivations are exactly the same as we did in the book. Since Vandermonde determinants are nonzero, δ columns of $\mathbf{H}_1$ can not be sum to zero. Hence the minimum distance of the extended RS code is at least $2t+1$. However, $\mathbf{H}$ generates an RS code with minimum distance exactly $2t+1$. There are $2t+1$ columns in $\mathbf{H}$ (they are also in $\mathbf{H}_1$), which sum to zero. Therefore the minimum distance of the extended RS code is exactly $2t+1$.

7.13 Consider

$$\mathbf{v}(X) = \sum_{i=0}^{2^m-2} \mathbf{a}(\alpha^i)X^i = \sum_{i=0}^{2^m-2} (\sum_{j=0}^{k-1} a_j \alpha^{ij})X^i$$

Let α be a primitive element in GF(2^m). Replacing X by α^q, we have

$$\begin{aligned}\mathbf{v}(\alpha^q) &= \sum_{i=0}^{2^m-2}\sum_{j=0}^{k-1} a_j \alpha^{ij}\alpha^{iq} \\ &= \sum_{j=0}^{k-1} a_j (\sum_{i=0}^{2^m-2} \alpha^{i(j+q)}).\end{aligned}$$

We factor $1 + X^{2^-1}$ as follows:

$$1 + X^{2^m-1} = (1 + X)(1 + X + X^2 + \cdots + X^{2^m-2})$$

Since the polynomial $1 + X + X^2 + \cdots + X^{2^m-2}$ has α, α^2, $\ldots$, α^{2^m-2} as roots, then for $1 \leq l \leq 2^m - 2$,

$$\sum_{i=0}^{2^m-2} \alpha^{li} = 1 + \alpha^l + \alpha^{2l} + \cdots + \alpha^{(2^m-2)l} = 0.$$

Therefore,

$$\textstyle\sum_{i=0}^{2^m-2} \alpha^{i(j+q)} = 0 \qquad \text{when } 1 \leq j + q \leq 2^m - 2.$$

This implies that

$$\mathbf{v}(\alpha^q) = 0 \qquad \text{for } 0 \leq j < k \text{ and } 1 \leq q \leq 2^m - k - 1.$$

Hence $\mathbf{v}(X)$ has α, α^2, $\ldots$, α^{2^m-k-1} as roots. The set $\{$**v**(X)$\}$ is a set of polynomial over GF(2^m) with $2^m - k - 1$ consecutive powers of α as roots and hence it forms a $(2^m - 1, k, 2^m - k)$ cyclic RS code over GF(2^m).