Chapter 6

6.1 (a) The elements β, β^2 and β^4 have the same minimal polynomial $\phi_1(X)$. From table 2.9, we find that

$$\phi_1(X) = 1 + X^3 + X^4$$

The minimal polynomial of $\beta^3 = \alpha^{21} = \alpha^6$ is

$$\phi_3(X) = 1 + X + X^2 + X^3 + X^4.$$

Thus

$$\begin{aligned} \mathbf{g}_0(X) &= LCM(\phi_1(X), \phi_2(X)) \\ &= (1 + X^3 + X^4)(1 + X + X^2 + X^3 + X^4) \\ &= 1 + X + X^2 + X^4 + X^8. \end{aligned}$$

(b)

$$\mathbf{H} = \begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 & \beta^7 & \beta^8 & \beta^9 & \beta^{10} & \beta^{11} & \beta^{12} & \beta^{13} & \beta^{14} \\ 1 & \beta^3 & \beta^6 & \beta^9 & \beta^{12} & \beta^{15} & \beta^{18} & \beta^{21} & \beta^{24} & \beta^{27} & \beta^{30} & \beta^{33} & \beta^{36} & \beta^{39} & \beta^{42} \end{bmatrix}$$

$$\mathbf{H} = \left[\begin{array}{ccccccccccccccc} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ \hdashline 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

(c) The reciprocal of $\mathbf{g}(X)$ in Example 6.1 is

$$\begin{aligned} X^8\mathbf{g}(X^{-1}) &= X^8(1+X^{-4}+X^{-6}+X^{-7}+X^{-8} \\ &= X^8+X^4+X^2+X+1=\mathbf{g}_0(X) \end{aligned}$$

6.2 The table for $GF(s^5)$ with $p(X) = 1 + X^2 + X^5$ is given in Table P.6.2(a). The minimal polynomials of elements in $GF(2^m)$ are given in Table P.6.2(b). The generator polynomials of all the binary BCH codes of length 31 are given in Table P.6.2(c)

Table P.6.2(a) Galois Field GF(2^5) with $\mathbf{p}(\alpha) = 1 + \alpha^2 + \alpha^5 = 0$

0					(0 0 0 0 0)
1					(1 0 0 0 0)
α					(0 1 0 0 0)
α^2					(0 0 1 0 0)
α^3					(0 0 0 1 0)
α^4					(0 0 0 0 1)
α^5	=	1	+	α^2	(1 0 1 0 0)

Table P.6.2(a) Continued

α^6	=			α			+	α^3			(0 1 0 1 0)
α^7	=					α^2			+	α^4	(0 0 1 0 1)
α^8	=	1			+	α^2	+	α^3			(1 0 1 1 0)
α^9	=			α			+	α^3	+	α^4	(0 1 0 1 1)
α^{10}	=	1							+	α^4	(1 0 0 0 1)
α^{11}	=	1	+	α	+	α^2					(1 1 1 0 0)
α^{12}	=			α	+	α^2	+	α^3			(0 1 1 1 0)
α^{13}	=					α^2	+	α^3	+	α^4	(0 0 1 1 1)
α^{14}	=	1			+	α^2	+	α^3	+	α^4	(1 0 1 1 1)
α^{15}	=	1	+	α	+	α^2	+	α^3	+	α^4	(1 1 1 1 1)
α^{16}	=	1	+	α			+	α^3	+	α^4	(1 1 0 1 1)
α^{17}	=	1	+	α					+	α^4	(1 1 0 0 1)
α^{18}	=	1	+	α							(1 1 0 0 0)
α^{19}	=			α	+	α^2					(0 1 1 0 0)
α^{20}	=					α^2	+	α^3			(0 0 1 1 0)
α^{21}	=							α^3	+	α^4	(0 0 0 1 1)
α^{22}	=	1			+	α^2			+	α^4	(1 0 1 0 1)
α^{23}	=	1	+	α	+	α^2	+	α^3			(1 1 1 1 0)
α^{24}	=			α	+	α^2	+	α^3	+	α^4	(0 1 1 1 1)
α^{25}	=	1					+	α^3	+	α^4	(1 0 0 1 1)
α^{26}	=	1	+	α	+	α^2			+	α^4	(1 1 1 0 1)
α^{27}	=	1	+	α			+	α^3			(1 1 0 1 0)
α^{28}	=			α	+	α^2			+	α^4	(0 1 1 0 1)
α^{29}	=	1	+				+	α^3			(1 0 0 1 0)
α^{30}	=			α					+	α^4	(0 1 0 0 1)

Table P.6.2(b)

Conjugate Roots	$\phi_i(X)$
1	1 + X
$\alpha,\ \alpha^2,\ \alpha^4,\ \alpha^8,\ \alpha^{16}$	$1 + X^2 + X^5$
$\alpha^3,\ \alpha^6,\ \alpha^{12},\ \alpha^{24},\ \alpha^{17}$	$1 + X^2 + X^3 + X^4 + X^5$
$\alpha^5,\ \alpha^{10},\ \alpha^{20},\ \alpha^9,\ \alpha^{18}$	$1 + X + X^2 + X^4 + X^5$
$\alpha^7,\ \alpha^{14},\ \alpha^{28},\ \alpha^{25},\ \alpha^{19}$	$1 + X + X^2 + X^3 + X^5$
$\alpha^{11},\ \alpha^{22},\ \alpha^{13},\ \alpha^{26},\ \alpha^{21}$	$1 + X + X^3 + X^4 + X^5$
$\alpha^{15},\ \alpha^{30},\ \alpha^{29},\ \alpha^{27},\ \alpha^{23}$	$1 + X^3 + X^5$

Table P.6.2(c)

n	k	t	$\mathbf{g}(X)$
31	26	1	$\mathbf{g}_1(X) = 1 + X^2 + X^5$
	21	2	$\mathbf{g}_2(X) = \phi_1(X)\phi_3(X)$
	16	3	$\mathbf{g}_3(X) = \phi_1(X)\phi_3(X)\phi_5(X)$
	11	5	$\mathbf{g}_4(X) = \phi_1(X)\phi_3(X)\phi_5(X)\phi_7(X)$
	6	7	$\mathbf{g}_5(X) = \phi_1(X)\phi_3(X)\phi_5(X)\phi_7(X)\phi_{11}(X)$

6.3 (a) Use the table for $GF(2^5)$ constructed in Problem 6.2. The syndrome components of $\mathbf{r}_1(X) = X^7 + X^{30}$ are:

$$S_1 = \mathbf{r}_1(\alpha) = \alpha^7 + \alpha^{30} = \alpha^{19}$$

$$S_2 = \mathbf{r}_1(\alpha^2) = \alpha^{14} + \alpha^{29} = \alpha^7$$

$$S_3 = \mathbf{r}_1(\alpha^3) = \alpha^{21} + \alpha^{28} = \alpha^{12}$$

$$S_4 = \mathbf{r}_1(\alpha^4) = \alpha^{28} + \alpha^{27} = \alpha^{14}$$

The iterative procedure for finding the error location polynomial is shown in Table P.6.3(a)

Table P.6.3(a)

μ	$\sigma^{(\mu)}(X)$	d_μ	ℓ_μ	$2\mu - \ell_\mu$
-1/2	1	1	0	-1
0	1	α^{19}	0	0
1	$1 + \alpha^{19}X$	α^{25}	1	$1(\rho = -1/2)$
2	$1 + \alpha^{19}X + \alpha^6X^2$	–	2	$2(\rho = 0)$

Hence $\sigma(X) = 1 + \alpha^{19}X + \alpha^6X^2$. Substituting the nonzero elements of $GF(2^5)$ into $\sigma(X)$, we find that $\sigma(X)$ has α and α^{24} as roots. Hence the error location numbers are $\alpha^{-1} = \alpha^{30}$ and $\alpha^{-24} = \alpha^7$. As a result, the error polynomial is

$$\mathbf{e}(X) = X^7 + X^{30}.$$

The decoder decodes $\mathbf{r}_1(X)$ into $\mathbf{r}_1(X) + \mathbf{e}(X) = \mathbf{0}$.

(b) Now we consider the decoding of $\mathbf{r}_2(X) = 1 + X^{17} + X^{28}$. The syndrome components of $\mathbf{r}_2(X)$ are:

$$S_1 = \mathbf{r}_2(\alpha) = \alpha^2,$$

$$S_2 = S_1^2 = \alpha^4,$$

$$S_4 = S_2^2 = \alpha^8,$$

$$S_3 = \mathbf{r}_2(\alpha^3) = \alpha^{21}.$$

The error location polynomial $\sigma(X)$ is found by filling Table P.6.3(b):

Table P.6.3(b)

μ	$\sigma^{(\mu)}(X)$	d_μ	ℓ_μ	$2\mu - \ell_\mu$
-1/2	1	1	0	-1
0	1	α^2	0	0
1	$1 + \alpha^2 X$	α^{30}	1	1($\rho = -1/2$)
2	$1 + \alpha^2 X + \alpha^{28} X^2$	–	2	2($\rho = 0$)

The estimated error location polynomial is

$$\sigma(X) = 1 + \alpha^2 X + \alpha^{28} X^2$$

This polynomial does not have roots in $GF(2^5)$, and hence $\mathbf{r}_2(X)$ cannot be decoded and must contain more than two errors.

6.4 Let $n = (2t+1)\lambda$. Then

$$(X^n + 1) = (X^\lambda + 1)(X^{2t\lambda} + X^{(2t-1)\lambda} + \cdots + X^\lambda + 1$$

The roots of $X^\lambda + 1$ are 1, α^{2t+1}, $\alpha^{2(2t+1)}$, $\cdots$, $\alpha^{(\lambda-1)(2t+1)}$. Hence, α, α^2, $\cdots$, α^{2t} are roots of the polynomial

$$\mathbf{u}(X) = 1 + X^\lambda + X^{2\lambda} + \cdots + X^{(2t-1)\lambda} + X^{2t\lambda}.$$

This implies that $\mathbf{u}(X)$ is code polynomial which has weight $2t+1$. Thus the code has minimum distance exactly $2t+1$.

6.5 Consider the Galois field $GF(2^{2m})$. Note that $2^{2m} - 1 = (2^m - 1) \cdot (2^m + 1)$. Let α be a primitive element in $GF(2^{2m})$. Then $\beta = \alpha^{(2^m-1)}$ is an element of order $2^m + 1$. The elements $1, \beta, \beta^2, \beta^2, \beta^3, \beta^4, \cdots, \beta^{2m}$ are all the roots of $X^{2^m+1}+1$. Let $\psi_i(X)$ be the minimal polynomial of β^i. Then a t-error-correcting non-primitive BCH code of length $n = 2^m + 1$ is generated by

$$\mathbf{g}(X) = LCM\left\{\psi_1(X), \psi_2(X), \cdots, \psi_{2t}(X)\right\}.$$

6.10 Use Tables 6.2 and 6.3. The minimal polynomial for $\beta^2 = \alpha^6$ and $\beta^4 = \alpha^{12}$ is

$$\psi_2(X) = 1 + X + X^2 + X^4 + X^6.$$

The minimal polynomial for $\beta^3 = \alpha^9$ is

$$\psi_3(X) = 1 + X^2 + X^3.$$

The minimal polynomial for $\beta^5 = \alpha^{15}$ is

$$\psi_5(X) = 1 + X^2 + X^4 + X^5 + X^6.$$

Hence

$$\mathbf{g}(X) = \psi_2(X)\psi_3(X)\psi_5(X)$$

The orders of β^2, β^3 and β^5 are 21,7 and 21 respectively. Thus the length is

$$n = LCM(21, 7, 21),$$

and the code is a double-error-correcting (21,6) BCH code.

6.11 (a) Let $\mathbf{u}(X)$ be a code polynomial and $\mathbf{u}^*(X) = X^{n-1}\mathbf{u}(X^{-1})$ be the reciprocal of $\mathbf{u}(X)$. A cyclic code is said to be reversible if $\mathbf{u}(X)$ is a code polynomial then $\mathbf{u}^*(X)$ is also a code polynomial. Consider

$$\mathbf{u}^*(\beta^i) = \beta^{(n-1)i}\mathbf{u}(\beta^{-i})$$

Since $\mathbf{u}(\beta^{-i}) = 0$ for $-t \le i \le t$, we see that $\mathbf{u}^*(\beta^i)$ has $\beta^{-t}, \cdots, \beta^{-1}, \beta^0, \beta^1, \cdots, \beta^t$ as roots and is a multiple of the generator polynomial $\mathbf{g}(X)$. Therefore $\mathbf{u}^*(X)$ is a code polynomial.

(b) If t is odd, $t+1$ is even. Hence β^{t+1} is the conjugate of $\beta^{(t+1)/2}$ and $\beta^{-(t+1)}$ is the conjugate of $\beta^{-(t+1)/2}$. Thus β^{t+1} and $\beta^{-(t+1)}$ are also roots of the generator polynomial. It follows from the BCH bound that the code has minimum distance $2t+4$ (Since the generator polynomial has $(2t+3$ consecutive powers of β as roots).