Chapter 5

5.6 (a) A polynomial over GF(2) with odd number of terms is not divisible by $X + 1$, hence it can not be divisible by $\mathbf{g}(X)$ if $\mathbf{g}(X)$ has $(X + 1)$ as a factor. Therefore, the code contains no code vectors of odd weight.

(b) The polynomial $X^n + 1$ can be factored as follows:

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

Since $\mathbf{g}(X)$ divides $X^n + 1$ and since $\mathbf{g}(X)$ does not have $X + 1$ as a factor, $\mathbf{g}(X)$ must divide the polynomial $X^{n-1} + X^{n-2} + \cdots + X + 1$. Therefore $1 + X + \cdots + X^{n-2} + X^{n-1}$ is a code polynomial, the corresponding code vector consists of all $1'$s.

(c) First, we note that no X^i is divisible by $\mathbf{g}(X)$. Hence, no code word with weight one. Now, suppose that there is a code word $\mathbf{v}(X)$ of weight 2. This code word must be of the form,

$$\mathbf{v}(X) = X^i + X^j$$

with $0 \leq i < j < n$. Put $\mathbf{v}(X)$ into the following form:

$$\mathbf{v}(X) = X^i(1 + X^{j-i}).$$

Note that $\mathbf{g}(X)$ and X^i are relatively prime. Since $\mathbf{v}(X)$ is a code word, it must be divisible by $\mathbf{g}(X)$. Since $\mathbf{g}(X)$ and X^i are relatively prime, $\mathbf{g}(X)$ must divide the polynomial $X^{j-i}+1$. However, $j - i < n$. This contradicts the fact that n is the smallest integer such that $\mathbf{g}(X)$ divides $X^n + 1$. Hence our hypothesis that there exists a code vector of weight 2 is invalid. Therefore, the code has a minimum weight at least 3.

5.7 (a) Note that $X^n + 1 = \mathbf{g}(X)\mathbf{h}(X)$. Then

$$X^n(X^{-n} + 1) = X^n\mathbf{g}(X^{-1})\mathbf{h}(X^{-1})$$

$$1 + X^n = \left[X^{n-k}\mathbf{g}(X^{-1})\right]\left[X^k\mathbf{h}(X^{-1})\right]$$

$$= \mathbf{g}^*(X)\mathbf{h}^*(X).$$

where $\mathbf{h}^*(X)$ is the reciprocal of $\mathbf{h}(X)$. We see that $\mathbf{g}^*(X)$ is factor of $X^n + 1$. Therefore, $\mathbf{g}^*(X)$ generates an (n, k) cyclic code.

(b) Let C and C^* be two (n, k) cyclic codes generated by $\mathbf{g}(X)$ and $\mathbf{g}^*(X)$ respectively. Let $\mathbf{v}(X) = v_0 + v_1X + \cdots + v_{n-1}X^{n-1}$ be a code polynomial in C. Then $\mathbf{v}(X)$ must be a multiple of $\mathbf{g}(X)$, i.e.,

$$\mathbf{v}(X) = \mathbf{a}(X)\mathbf{g}(X).$$

Replacing X by X^{-1} and multiplying both sides of above equality by X^{n-1}, we obtain

$$X^{n-1}\mathbf{v}(X^{-1}) = \left[X^{k-1}\mathbf{a}(X^{-1})\right]\left[X^{n-k}\mathbf{g}(X^{-1})\right]$$

Note that $X^{n-1}\mathbf{v}(X^{-1})$, $X^{k-1}\mathbf{a}(X^{-1})$ and $X^{n-k}\mathbf{g}(X^{-1})$ are simply the reciprocals of $\mathbf{v}(X)$, $\mathbf{a}(X)$ and $\mathbf{g}(X)$ respectively. Thus,

$$\mathbf{v}^*(X) = \mathbf{a}^*(X)\mathbf{g}^*(X). \quad (1)$$

From (1), we see that the reciprocal $\mathbf{v}^*(X)$ of a code polynomial in C is a code polynomial in C^*. Similarly, we can show the reciprocal of a code polynomial in C^* is a code polynomial in C. Since $\mathbf{v}^*(X)$ and $\mathbf{v}(X)$ have the same weight, C^* and C have the same weight distribution.

5.8 Let C_1 be the cyclic code generated by $(X + 1)\mathbf{g}(X)$. We know that C_1 is a subcode of C and C_1 consists all the even-weight code vectors of C as all its code vectors. Thus the weight enumerator $A_1(z)$ of C_1 should consists of only the even-power terms of $A(z) = \sum_{i=0}^{n} A_i z^i$. Hence

$$A_1(z) = \sum_{j=0}^{\lfloor n/2 \rfloor} A_{2j} z^{2j} \quad (1)$$

Consider the sum

$$A(z) + A(-z) = \sum_{i=0}^{n} A_i z^i + \sum_{i=0}^{n} A_i (-z)^i$$

$$= \sum_{i=0}^{n} A_i \left[z^i + (-z)^i \right].$$

We see that $z^i + (-z)^i = 0$ if i is odd and that $z^i + (-z)^i = 2z^i$ if i is even. Hence

$$A(z) + A(-z) = \sum_{j=0}^{\lfloor n/2 \rfloor} 2A_{2j} z^{2j} \tag{2}$$

From (1) and (2), we obtain

$$A_1(z) = 1/2 \left[A(z) + A(-z) \right].$$

5.10 Let $\mathbf{e}_1(X) = X^i + X^{i+1}$ and $\mathbf{e}_2(X) = X^j + X^{j+1}$ be two different double-adjacent-error patterns such that $i < j$. Suppose that $\mathbf{e}_1(X)$ and $\mathbf{e}_2(X)$ are in the same coset. Then $\mathbf{e}_1(X) + \mathbf{e}_2(X)$ should be a code polynomial and is divisible by $\mathbf{g}(X) = (X+1)\mathbf{p}(X)$. Note that

$$\mathbf{e}_1(X) + \mathbf{e}_2(X) = X^i(X+1) + X^j(X+1)$$

$$= (X+1)X^i(X^{j-i}+1)$$

Since $\mathbf{g}(X)$ divides $\mathbf{e}_1(X) + \mathbf{e}_2(X)$, $\mathbf{p}(X)$ should divide $X^i(X^{j-i}+1)$. However $\mathbf{p}(X)$ and X^i are relatively prime. Therefore $\mathbf{p}(X)$ must divide $X^{j-i}+1$. This is not possible since $j - i < 2^m - 1$ and $\mathbf{p}(X)$ is a primitive polynomial of degree m (the smallest integer n such that $\mathbf{p}(X)$ divides $X^n + 1$ is $2^m - 1$). Thus $\mathbf{e}_1(X) + \mathbf{e}_2(X)$ can not be in the same coset.

5.12 Note that $\mathbf{e}^{(i)}(X)$ is the remainder resulting from dividing $X^i\mathbf{e}(X)$ by $X^n + 1$. Thus

$$X^i\mathbf{e}(X) = \mathbf{a}(X)(X^n+1) + \mathbf{e}^{(i)}(X) \tag{1}$$

Note that $\mathbf{g}(X)$ divides $X^n + 1$, and $\mathbf{g}(X)$ and X^i are relatively prime. From (1), we see that if $\mathbf{e}(X)$ is not divisible by $\mathbf{g}(X)$, then $\mathbf{e}^{(i)}(X)$ is not divisible by $\mathbf{g}(X)$. Therefore, if $\mathbf{e}(X)$ is detectable, $\mathbf{e}^{(i)}(X)$ is also detectable.

5.14 Suppose that ℓ does not divide n. Then

$$n = k \cdot \ell + r, \quad 0 < r < \ell.$$

Note that

$$\mathbf{v}^{(n)}(X) = \mathbf{v}^{(k \cdot \ell + r)}(X) = \mathbf{v}(X) \tag{1}$$

Since $\mathbf{v}^{(\ell)}(X) = \mathbf{v}(X)$,

$$\mathbf{v}^{(k \cdot \ell)}(X) = \mathbf{v}(X) \tag{2}$$

From (1) and (2), we have

$$\mathbf{v}^{(r)}(X) = \mathbf{v}(X).$$

This is not possible since $0 < r < \ell$ and ℓ is the smallest positive integer such that $\mathbf{v}^{(\ell)}(X) = \mathbf{v}(X)$. Therefore, our hypothesis that ℓ does not divide n is invalid, hence ℓ must divide n.

5.17 Let n be the order of β. Then $\beta^n = 1$, and β is a root of $X^n + 1$. It follows from Theorem 2.14 that $\phi(X)$ is a factor of $X^n + 1$. Hence $\phi(X)$ generates a cyclic code of length n.

5.18 Let n_1 be the order of β_1 and n_2 be the order of β_2. Let n be the least common multiple of n_1 and n_2, i.e. $n = LCM(n_1, n_2)$. Consider $X^n + 1$. Clearly, β_1 and β_2 are roots of $X^n + 1$. Since $\phi_1(X)$ and $\phi_2(X)$ are factors of $X^n + 1$. Since $\phi_1(X)$ and $\phi_2(X)$ are relatively prime, $\mathbf{g}(X) = \phi_1(X) \cdot \phi_2(X)$ divides $X^n + 1$. Hence $\mathbf{g}(X) = \phi_1(X) \cdot \phi_2(X)$ generates a cyclic code of length $n = LCM(n_1, n_2)$.

5.19 Since every code polynomial $\mathbf{v}(X)$ is a multiple of the generator polynomial $\mathbf{p}(X)$, every root of $\mathbf{p}(X)$ is a root of $\mathbf{v}(X)$. Thus $\mathbf{v}(X)$ has α and its conjugates as roots. Suppose $\mathbf{v}(X)$ is a binary polynomial of degree $2^m - 2$ or less that has α as a root. It follows from Theorem 2.14 that $\mathbf{v}(X)$ is divisible by the minimal polynomial $\mathbf{p}(X)$ of α. Hence $\mathbf{v}(X)$ is a code polynomial in the Hamming code generated by $\mathbf{p}(X)$.

5.20 Let $\mathbf{v}(X)$ be a code polynomial in both C_1 and C_2. Then $\mathbf{v}(X)$ is divisible by both $\mathbf{g}_1(X)$ and $\mathbf{g}_2(X)$. Hence $\mathbf{v}(X)$ is divisible by the least common multiple $\mathbf{g}(X)$ of $\mathbf{g}_1(X)$ and $\mathbf{g}_2(X)$, i.e. $\mathbf{v}(X)$ is a multiple of $\mathbf{g}(X) = LCM(\mathbf{g}_1(X), \mathbf{g}_2(X))$. Conversely, any polynomial of degree $n - 1$ or less that is a multiple of $\mathbf{g}(X)$ is divisible by $\mathbf{g}_1(X)$ and $\mathbf{g}_2(X)$. Hence $\mathbf{v}(X)$ is in both C_1 and C_2. Also we note that $\mathbf{g}(X)$ is a factor of $X^n + 1$. Thus the code polynomials common to C_1 and C_2 form a cyclic code of length n whose generator polynomial is $\mathbf{g}(X) = LCM(\mathbf{g}_1(X), \mathbf{g}_2(X))$. The code C_3 generated by $\mathbf{g}(X)$ has minimum distance $d_3 \geq max(d_1, d_2)$.

5.21 See Problem 4.3.

5.22 (a) First, we note that $X^{2^m-1} + 1 = \mathbf{p}^*(X)\mathbf{h}^*(X)$. Since the roots of $X^{2^m-1} + 1$ are the $2^m - 1$ nonzero elements in GF(2^m) which are all distinct, $\mathbf{p}^*(X)$ and $\mathbf{h}^*(X)$ are relatively prime. Since every code polynomial $\mathbf{v}(X)$ in C_d is a polynomial of degree $2^m - 2$ or less, $\mathbf{v}(X)$ can not be divisible by $\mathbf{p}(X)$ (otherwise $\mathbf{v}(X)$ is divisible by $\mathbf{p}^*(X)\mathbf{h}^*(X) = X^{2^m-1}+1$ and has degree at least $2^m - 1$). Suppose that $\mathbf{v}^{(i)}(X) = \mathbf{v}(X)$. It follows from (5.1) that

$$X^i\mathbf{v}(X) = \mathbf{a}(X)(X^{2^m-1} + 1) + \mathbf{v}^{(i)}(X)$$

$$= \mathbf{a}(X)(X^{2^m-1} + 1) + \mathbf{v}(X)$$

Rearranging the above equality, we have

$$(X^i + 1)\mathbf{v}(X) = \mathbf{a}(X)(X^{2^m-1} + 1).$$

Since $\mathbf{p}(X)$ divides $X^{2^m-1} + 1$, it must divide $(X^i + 1)\mathbf{v}(X)$. However $\mathbf{p}(X)$ and $\mathbf{v}(X)$ are relatively prime. Hence $\mathbf{p}(X)$ divides $X^i + 1$. This is not possible since $0 < i < 2^m - 1$ and $\mathbf{p}(X)$ is a primitive polynomial(the smallest positive integer n such that $\mathbf{p}(X)$ divides $X^n + 1$ is $n = 2^m - 1$). Therefore our hypothesis that, for $0 < i < 2^m - 1$, $\mathbf{v}^{(i)}(X) = \mathbf{v}(X)$ is invalid, and $\mathbf{v}^{(i)}(X) \neq \mathbf{v}(X)$.

(b) From part (a), a code polynomial $\mathbf{v}(X)$ and its $2^m - 2$ cyclic shifts form all the $2^m - 1$ nonzero code polynomials in C_d. These $2^m - 1$ nonzero code polynomial have the same weight, say w. The total number of nonzero components in the code words of C_d is $w \cdot (2^m - 1)$. Now we arrange the 2^m code words in C_d as an $2^m \times (2^m - 1)$ array. It follows from Problem 3.6(b) that every column in this array has exactly 2^{m-1} nonzero components. Thus the total nonzero components in the array is $2^{m-1} \cdot (2^m - 1)$. Equating $w.(2^m - 1)$ to $2^{m-1} \cdot (2^m - 1)$, we have

$$w = 2^{m-1}.$$

5.25 (a) Any error pattern of double errors must be of the form,

$$\mathbf{e}(X) = X^i + X^j$$

where $j > i$. If the two errors are not confined to $n - k = 10$ consecutive positions, we must have

$$j - i + 1 > 10,$$

$$15 - (j - i) + 1 > 10.$$

Simplifying the above inequalities, we obtain

$$j - i > 9$$

$$j - i < 6.$$

This is impossible. Therefore any double errors are confined to 10 consecutive positions and can be trapped.

(b) An error pattern of triple errors must be of the form,

$$\mathbf{e}(X) = X^i + X^j + X^k,$$

where $0 \leq i < j < k \leq 14$. If these three errors can not be trapped, we must have

$$k - i > 9$$

$$j - i < 6$$

$$k - j < 6.$$

If we fix i, the only solutions for j and k are $j = 5 + i$ and $k = 10 + i$. Hence, for three errors not confined to 10 consecutive positions, the error pattern must be of the following form

$$\mathbf{e}(X) = X^i + X^{5+i} + X^{10+i}$$

for $0 \leq i < 5$. Therefore, only 5 error patterns of triple errors can not be trapped.

5.26 (b) Consider a double-error pattern,

$$\mathbf{e}(X) = X^i + X^j$$

where $0 \leq i < j < 23$. If these two errors are not confined to 11 consecutive positions, we must have

$$j - i + 1 > 11$$

$$23 - (j - i - 1) > 11$$

From the above inequalities, we obtain

$$10 < j - i < 13$$

For a fixed i, j has two possible solutions, $j = 11+i$ and $j = 12+i$. Hence, for a double-error pattern that can not be trapped, it must be either of the following two forms:

$$\mathbf{e}_1(X) = X^i + X^{11+i},$$

$$\mathbf{e}_1(X) = X^i + X^{12+i}.$$

There are a total of 23 error patterns of double errors that can not be trapped.

5.27 The coset leader weight distribution is

$$\alpha_0 = 1, \alpha_1 = \binom{23}{1}, \alpha_2 = \binom{23}{2}, \alpha_3 = \binom{23}{3}$$

$$\alpha_4 = \alpha_5 = \cdots = \alpha_{23} = 0$$

The probability of a correct decoding is

$$P(C) = (1-p)^{23} + \binom{23}{1} p(1-p)^{22} + \binom{23}{2} p^2(1-p)^{21}$$

$$+\binom{23}{3}p^3(1-p)^{20}.$$

The probability of a decoding error is

$$P(E) = 1 - P(C).$$

5.29(a) Consider two single-error patterns, $\mathbf{e}_1(X) = X^i$ and $\mathbf{e}_2(X) = X^j$, where $j > i$. Suppose that these two error patterns are in the same coset. Then $X^i + X^j$ must be divisible by $\mathbf{g}(X) = (X^3 + 1)\mathbf{p}(X)$. This implies that $X^{j-i} + 1$ must be divisible by $\mathbf{p}(X)$. This is impossible since $j - i < n$ and n is the smallest positive integer such that $\mathbf{p}(X)$ divides $X^n + 1$. Therefore no two single-error patterns can be in the same coset. Consequently, all single-error patterns can be used as coset leaders.

Now consider a single-error pattern $\mathbf{e}_1(X) = X^i$ and a double-adjacent-error pattern $\mathbf{e}_2(X) = X^j + X^{j+1}$, where $j > i$. Suppose that $\mathbf{e}_1(X)$ and $\mathbf{e}_2(X)$ are in the same coset. Then $X^i + X^j + X^{j+1}$ must be divisible by $\mathbf{g}(X) = (X^3+1)\mathbf{p}(X)$. This is not possible since $\mathbf{g}(X)$ has $X + 1$ as a factor, however $X^i + X^j + X^{j+1}$ does not have $X + 1$ as a factor. Hence no single-error pattern and a double-adjacent-error pattern can be in the same coset.

Consider two double-adjacent-error patterns,$X^i + X^{i+1}$ and $X^j + X^{j+1}$ where $j > i$. Suppose that these two error patterns are in the same cosets. Then $X^i + X^{i+1} + X^j + X^{j+1}$ must be divisible by $(X^3 + 1)\mathbf{p}(X)$. Note that

$$X^i + X^{i+1} + X^j + X^{j+1} = X^i(X + 1)(X^{j-i} + 1).$$

We see that for $X^i(X + 1)(X^{j-i} + 1)$ to be divisible by $\mathbf{p}(X)$, $X^{j-i} + 1$ must be divisible by $\mathbf{p}(X)$. This is again not possible since $j - i < n$. Hence no two double-adjacent-error patterns can be in the same coset.

Consider a single error pattern X^i and a triple-adjacent-error pattern $X^j + X^{j+1} + X^{j+2}$. If these two error patterns are in the same coset, then $X^i + X^j + X^{j+1} + X^{j+2}$ must be divisible by $(X^3 + 1)\mathbf{p}(X)$. But $X^i + X^j + X^{j+1} + X^{j+2} = X^i + X^j(1 + X + X^2)$ is not divisible by $X^3 + 1 = (X + 1)(X^2 + X + 1)$. Therefore, no single-error pattern and a triple-adjacent-error pattern can be in the same coset.

Now we consider a double-adjacent-error pattern $X^i + X^{i+1}$ and a triple-adjacent-error pattern

$X^j + X^{j+1} + X^{j+2}$. Suppose that these two error patterns are in the same coset. Then

$$X^i + X^{i+1} + X^j + X^{j+1} + X^{j+2} = X^i(X+1) + X^j(X^2 + X + 1)$$

must be divisible by $(X^3+1)\mathbf{p}(X)$. This is not possible since $X^i+X^{i+1}+X^j+X^{j+1}+X^{j+2}$ does not have $X+1$ as a factor but X^3+1 has $X+1$ as a factor. Hence a double-adjacent-error pattern and a triple-adjacent-error pattern can not be in the same coset.

Consider two triple-adjacent-error patterns, $X^i + X^{i+1} + X^{i+2}$ and $X^j + X^{j+1} + X^{j+2}$. If they are in the same coset, then their sum

$$X^i(X^2 + X + 1)(1 + X^{j-i})$$

must be divisible by $(X^3 + 1)\mathbf{p}(X)$, hence by $\mathbf{p}(X)$. Note that the degree of $\mathbf{p}(X)$ is 3 or greater. Hence $\mathbf{p}(X)$ and $(X^2 + X + 1)$ are relatively prime. As a result, $\mathbf{p}(X)$ must divide $X^{j-i} + 1$. Again this is not possible. Hence no two triple-adjacent-error patterns can be in the same coset.

Summarizing the above results, we see that all the single-, double-adjacent-, and triple-adjacent-error patterns can be used as coset leaders.