Chapter 2

2.3 Since m is not a prime, it can be factored as the product of two integers a and b,

$$m = a \cdot b$$

with $1 < a, b < m$. It is clear that both a and b are in the set $\{1, 2, \cdots, m-1\}$. It follows from the definition of modulo-m multiplication that

$$a \boxdot b = 0.$$

Since 0 is not an element in the set $\{1, 2, \cdots, m-1\}$, the set is not closed under the modulo-m multiplication and hence can not be a group.

2.5 It follows from Problem 2.3 that, if m is not a prime, the set $\{1, 2, \cdots, m-1\}$ can not be a group under the modulo-m multiplication. Consequently, the set $\{0, 1, 2, \cdots, m-1\}$ can not be a field under the modulo-m addition and multiplication.

2.7 First we note that the set of sums of unit element contains the zero element 0. For any $1 \leq \ell < \lambda$,

$$\sum_{i=1}^{\ell} 1 + \sum_{i=1}^{\lambda-\ell} 1 = \sum_{i=1}^{\lambda} 1 = 0.$$

Hence every sum has an inverse with respect to the addition operation of the field GF(q). Since the sums are elements in GF(q), they must satisfy the associative and commutative laws with respect to the addition operation of GF(q). Therefore, the sums form a commutative group under the addition of GF(q).

Next we note that the sums contain the unit element 1 of GF(q). For each nonzero sum

$$\sum_{i=1}^{\ell} 1$$

with $1 \leq \ell < \lambda$, we want to show it has a multiplicative inverse with respect to the multiplication operation of GF(q). Since λ is prime, ℓ and λ are relatively prime and there exist two integers a and b such that

$$a \cdot \ell + b \cdot \lambda = 1, \tag{1}$$

where a and λ are also relatively prime. Dividing a by λ, we obtain

$$a = k\lambda + r \quad with \quad 0 \leq r < \lambda. \tag{2}$$

Since a and λ are relatively prime, $r \neq 0$. Hence

$$1 \leq r < \lambda$$

Combining (1) and (2), we have

$$\ell \cdot r = -(b + k\ell) \cdot \lambda + 1$$

Consider

$$\begin{aligned} \sum_{i=1}^{\ell} 1 \cdot \sum_{i=1}^{r} 1 &= \sum_{i=1}^{\ell \cdot r} 1 = \sum_{i=1}^{-(b+k\ell)\cdot\lambda} +1 \\ &= (\sum_{i=1}^{\lambda} 1)(\sum_{i=1}^{-(b+k\ell)} 1) + 1 \\ &= 0 + 1 = 1. \end{aligned}$$

Hence, every nonzero sum has an inverse with respect to the multiplication operation of GF(q). Since the nonzero sums are elements of GF(q), they obey the associative and commutative laws with respect to the multiplication of GF(q). Also the sums satisfy the distributive law. As a result, the sums form a field, a subfield of GF(q).

2.8 Consider the finite field GF(q). Let n be the maximum order of the nonzero elements of GF(q) and let α be an element of order n. It follows from Theorem 2.9 that n divides $q - 1$, i.e.

$$q - 1 = k \cdot n.$$

Thus $n \leq q - 1$. Let β be any other nonzero element in GF(q) and let e be the order of β.

Suppose that e does not divide n. Let (n, e) be the greatest common factor of n and e. Then $e/(n, e)$ and n are relatively prime. Consider the element

$$\beta^{(n,e)}$$

This element has order $e/(n, e)$. The element

$$\alpha\beta^{(n,e)}$$

has order $ne/(n, e)$ which is greater than n. This contradicts the fact that n is the maximum order of nonzero elements in GF(q). Hence e must divide n. Therefore, the order of each nonzero element of GF(q) is a factor of n. This implies that each nonzero element of GF(q) is a root of the polynomial

$$X^n - 1.$$

Consequently, $q - 1 \leq n$. Since $n \leq q - 1$ (by Theorem 2.9), we must have

$$n = q - 1.$$

Thus the maximum order of nonzero elements in GF(q) is q-1. The elements of order $q - 1$ are then primitive elements.

2.11 (a) Suppose that $f(X)$ is irreducible but its reciprocal $f^*(X)$ is not. Then

$$f^*(X) = a(X) \cdot b(X)$$

where the degrees of $a(X)$ and $b(X)$ are nonzero. Let k and m be the degrees of $a(X)$ and $b(X)$ respectivly. Clearly, $k + m = n$. Since the reciprocal of $f^*(X)$ is $f(X)$,

$$f(X) = X^n f^*(\frac{1}{X}) = X^k a(\frac{1}{X}) \cdot X^m b(\frac{1}{X}).$$

This says that $f(X)$ is not irreducible and is a contradiction to the hypothesis. Hence $f^*(X)$ must be irreducible. Similarly, we can prove that if $f^*(X)$ is irreducible, $f(X)$ is also irreducible. Consequently, $f^*(X)$ is irreducible if and only if $f(X)$ is irreducible.

(b) Suppose that $f(X)$ is primitive but $f^*(X)$ is not. Then there exists a positive integer k less than $2^n - 1$ such that $f^*(X)$ divides $X^k + 1$. Let

$$X^k + 1 = f^*(X)q(X).$$

Taking the reciprocals of both sides of the above equality, we have

$$\begin{aligned} X^k + 1 &= X^k f^*(\frac{1}{X})q(\frac{1}{X}) \\ &= X^n f^*(\frac{1}{X}) \cdot X^{k-n} q(\frac{1}{X}) \\ &= f(X) \cdot X^{k-n} q(\frac{1}{X}). \end{aligned}$$

This implies that $f(X)$ divides $X^k + 1$ with $k < 2^n - 1$. This is a contradiction to the hypothesis that $f(X)$ is primitive. Hence$f^*(X)$ must be also primitive. Similarly, if $f^*(X)$ is primitive, $f(X)$ must also be primitive. Consequently $f^*(X)$ is primitive if and only if $f(X)$ is primitive.

2.15 We only need to show that $\beta, \beta^2, \cdots, \beta^{2^{e-1}}$ are distinct. Suppose that

$$\beta^{2^i} = \beta^{2^j}$$

for $0 \leq i, j < e$ and $i < j$. Then,

$$(\beta^{2^{j-i}-1})^{2^i} = 1.$$

Since the order β is a factor of $2^m - 1$, it must be odd. For $(\beta^{2^{j-i}-1})^{2^i} = 1$, we must have

$$\beta^{2^{j-i}-1} = 1.$$

Since both i and j are less than e, $j - i < e$. This is contradiction to the fact that the e is the smallest nonnegative integer such that

$$\beta^{2^e - 1} = 1.$$

Hence $\beta^{2^i} \neq \beta^{2^j}$ for $0 \leq i, j < e$.

2.16 Let n' be the order of β^{2^i}. Then

$$(\beta^{2^i})^{n'} = 1$$

Hence

$$(\beta^{n'})^{2^i} = 1. \tag{1}$$

Since the order n of β is odd, n and 2^i are relatively prime. From(1), we see that n divides n' and

$$n' = kn. \tag{2}$$

Now consider

$$(\beta^{2^i})^n = (\beta^n)^{2^i} = 1$$

This implies that n' (the order of β^{2^i}) divides n. Hence

$$n = \ell n' \tag{3}$$

From (2) and (3), we conclude that

$$n' = n.$$

2.20 Note that $c \cdot \mathbf{v} = c \cdot (\mathbf{0} + \mathbf{v}) = c \cdot \mathbf{0} + c \cdot \mathbf{v}$. Adding $-(c \cdot \mathbf{v})$ to both sides of the above equality, we have

$$\begin{aligned} c \cdot \mathbf{v} + [-(c \cdot \mathbf{v})] &= c \cdot \mathbf{0} + c \cdot \mathbf{v} + [-(c \cdot \mathbf{v})] \\ \mathbf{0} &= c \cdot \mathbf{0} + \mathbf{0}. \end{aligned}$$

Since $\mathbf{0}$ is the additive identity of the vector space, we then have

$$c \cdot \mathbf{0} = \mathbf{0}.$$

2.21 Note that $0 \cdot \mathbf{v} = \mathbf{0}$. Then for any c in F,

$$(-c + c) \cdot \mathbf{v} = \mathbf{0}$$

$$(-c)\cdot\mathbf{v}+c\cdot\mathbf{v}=\mathbf{0}.$$

Hence $(-c)\cdot\mathbf{v}$ is the additive inverse of $c\cdot\mathbf{v}$, i.e.

$$-(c\cdot\mathbf{v})=(-c)\cdot\mathbf{v} \tag{1}$$

Since $c\cdot\mathbf{0}=\mathbf{0}$ (problem 2.20),

$$c\cdot(-\mathbf{v}+\mathbf{v})=\mathbf{0}$$

$$c\cdot(-\mathbf{v})+c\cdot\mathbf{v}=\mathbf{0}.$$

Hence $c\cdot(-\mathbf{v})$ is the additive inverse of $c\cdot\mathbf{v}$, i.e.

$$-(c\cdot\mathbf{v})=c\cdot(-\mathbf{v}) \tag{2}$$

From (1) and (2), we obtain

$$-(c\cdot\mathbf{v})=(-c)\cdot\mathbf{v}=c\cdot(-\mathbf{v})$$

2.22 By Theorem 2.22, S is a subspace if (i) for any $\mathbf{u}$ and $\mathbf{v}$ in S, $\mathbf{u}+\mathbf{v}$ is in S and (ii) for any c in F and $\mathbf{u}$ in S, $c\cdot\mathbf{u}$ is in S. The first condition is now given, we only have to show that the second condition is implied by the first condition for $F=GF(2)$. Let $\mathbf{u}$ be any element in S. It follows from the given condition that

$$\mathbf{u}+\mathbf{u}=\mathbf{0}$$

is also in S. Let c be an element in GF(2). Then, for any $\mathbf{u}$ in S,

$$c\cdot\mathbf{u}=\begin{cases}\mathbf{0} & for \quad c=0\\ \mathbf{u} & for \quad c=1\end{cases}$$

Clearly $c\cdot\mathbf{u}$ is also in S. Hence S is a subspace.

2.24 If the elements of GF(2^m) are represented by m-tuples over GF(2), the proof that GF(2^m) is a vector space over GF(2) is then straight-forward.

2.27 Let $\mathbf{u}$ and $\mathbf{v}$ be any two elements in $S_1 \cap S_2$. It is clear the $\mathbf{u}$ and $\mathbf{v}$ are elements in S_1, and $\mathbf{u}$ and $\mathbf{v}$ are elements in S_2. Since S_1 and S_2 are subspaces,

$$\mathbf{u} + \mathbf{v} \in S_1$$

and

$$\mathbf{u} + \mathbf{v} \in S_2.$$

Hence,$\mathbf{u} + \mathbf{v}$ is in $S_1 \cap S_2$. Now let $\mathbf{x}$ be any vector in $S_1 \cap S_2$. Then $\mathbf{x} \in S_1$, and $\mathbf{x} \in S_2$. Again, since S_1 and S_2 are subspaces, for any c in the field F, $c \cdot \mathbf{x}$ is in S_1 and also in S_2. Hence $c \cdot \mathbf{v}$ is in the intersection, $S_1 \cap S_2$. It follows from Theorem 2.22 that $S_1 \cap S_2$ is a subspace.

Chapter 3

3.1 The generator and parity-check matrices are:

$$\mathbf{G} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

From the parity-check matrix we see that each column contains odd number of ones, and no two columns are alike. Thus no two columns sum to zero and any three columns sum to a 4-tuple with odd number of ones. However, the first, the second, the third and the sixth columns sum to zero. Therefore, the minimum distance of the code is 4.

3.4 (a) The matrix $\mathbf{H}_1$ is an $(n-k+1) \times (n+1)$ matrix. First we note that the $n-k$ rows of $\mathbf{H}$ are linearly independent. It is clear that the first $(n-k)$ rows of $\mathbf{H}_1$ are also linearly independent. The last row of $\mathbf{H}_1$ has a $''1''$ at its first position but other rows of $\mathbf{H}_1$ have a $''0''$ at their first position. Any linear combination including the last row of $\mathbf{H}_1$ will never yield a zero vector. Thus all the rows of $\mathbf{H}_1$ are linearly independent. Hence the row space of $\mathbf{H}_1$ has dimension $n-k+1$. The dimension of its null space, C_1, is then equal to

$$dim(C_1) = (n+1) - (n-k+1) = k$$

Hence C_1 is an $(n+1, k)$ linear code.

(b) Note that the last row of $\mathbf{H}_1$ is an all-one vector. The inner product of a vector with odd weight and the all-one vector is $''1''$. Hence, for any odd weight vector **v**,

$$\mathbf{v} \cdot \mathbf{H}_1^T \neq \mathbf{0}$$

and **v** cannot be a code word in C_1. Therefore, C_1 consists of only even-weight code words.

(c) Let **v** be a code word in C. Then $\mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$. Extend **v** by adding a digit v_∞ to its left.

This results in a vector of $n+1$ digits,

$$\mathbf{v}_1 = (v_\infty, \mathbf{v}) = (v_\infty, v_0, v_1, \cdots, v_{n-1}).$$

For $\mathbf{v}_1$ to be a vector in C_1, we must require that

$$\mathbf{v}_1\mathbf{H}_1^T = \mathbf{0}.$$

First we note that the inner product of $\mathbf{v}_1$ with any of the first $n-k$ rows of $\mathbf{H}_1$ is 0. The inner product of $\mathbf{v}_1$ with the last row of $\mathbf{H}_1$ is

$$v_\infty + v_0 + v_1 + \cdots + v_{n-1}.$$

For this sum to be zero, we must require that $v_\infty = 1$ if the vector $\mathbf{v}$ has odd weight and $v_\infty = 0$ if the vector $\mathbf{v}$ has even weight. Therefore, any vector $\mathbf{v}_1$ formed as above is a code word in C_1, there are 2^k such code words. The dimension of C_1 is k, these 2^k code words are all the code words of C_1.

3.5 Let C_e be the set of code words in C with even weight and let C_o be the set of code words in C with odd weight. Let **x** be any odd-weight code vector from C_o. Adding **x** to each vector in C_o, we obtain a set of C_e' of even weight vector. The number of vectors in C_e' is equal to the number of vectors in C_o, i.e. $|C_e'| = |C_o|$. Also $C_e' \subseteq C_e$. Thus,

$$|C_o| \leq |C_e| \qquad (1)$$

Now adding **x** to each vector in C_e, we obtain a set C_o' of odd weight code words. The number of vectors in C_o' is equal to the number of vectors in C_e and

$$C_o' \subseteq C_o$$

Hence

$$|C_e| \leq |C_o| \qquad (2)$$

From (1) and (2), we conclude that $|C_o| = |C_e|$.

3.6 (a) From the given condition on $\mathbf{G}$, we see that, for any digit position, there is a row in $\mathbf{G}$ with a nonzero component at that position. This row is a code word in C. Hence in the code array, each column contains at least one nonzero entry. Therefore no column in the code array contains only zeros.

(b) Consider the ℓ-th column of the code array. From part (a) we see that this column contains at least one $''1''$. Let S_0 be the code words with a $''0''$ at the ℓ-th position and S_1 be the codewords with a $''1''$ at the ℓ-th position. Let $\mathbf{x}$ be a code word from S_1. Adding $\mathbf{x}$ to each vector in S_0, we obtain a set S_1' of code words with a $''1''$ at the ℓ-th position. Clearly,

$$|S_1'| = |S_0| \tag{1}$$

and

$$S_1' \subseteq S_1. \tag{2}$$

Adding $\mathbf{x}$ to each vector in S_1, we obtain a set of S_0' of code words with a $''0''$ at the ℓ-th location. We see that

$$|S_0'| = |S_1| \tag{3}$$

and

$$S_0' \subseteq S_0. \tag{4}$$

From (1) and (2), we obtain

$$|S_0| \leq |S_1|. \tag{5}$$

From (3) and (4) ,we obtain

$$|S_1| \leq |S_0|. \tag{6}$$

From (5) and (6) we have $|S_0| = |S_1|$. This implies that the ℓ-th column of the code array consists 2^{k-1} zeros and 2^{k-1} ones.

(c) Let S_0 be the set of code words with a $''0''$ at the ℓ-th position. From part (b), we see that S_0 consists of 2^{k-1} code words. Let $\mathbf{x}$ and $\mathbf{y}$ be any two code words in S_0. The sum $\mathbf{x}+\mathbf{y}$ also has a zero at the ℓ-th location and hence is code word in S_0. Therefore S_0 is a subspace of the vector space of all n-tuples over GF(2). Since S_0 is a subset of C, it is a subspace of C. The dimension of S_0 is $k-1$.

3.7 Let $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ be any three n-tuples over GF(2). Note that

$$\begin{aligned} d(\mathbf{x},\mathbf{y}) &= w(\mathbf{x}+\mathbf{y}), \\ d(\mathbf{y},\mathbf{z}) &= w(\mathbf{y}+\mathbf{z}), \\ d(\mathbf{x},\mathbf{z}) &= w(\mathbf{x}+\mathbf{z}). \end{aligned}$$

It is easy to see that

$$w(\mathbf{u}) + w(\mathbf{v}) \geq w(\mathbf{u}+\mathbf{v}). \tag{1}$$

Let $\mathbf{u} = \mathbf{x}+\mathbf{y}$ and $\mathbf{v} = \mathbf{y}+\mathbf{z}$. It follows from (1) that

$$w(\mathbf{x}+\mathbf{y}) + w(\mathbf{y}+\mathbf{z}) \geq w(\mathbf{x}+\mathbf{y}+\mathbf{y}+\mathbf{z}) = w(\mathbf{x}+\mathbf{z}).$$

From the above inequality, we have

$$d(\mathbf{x},\mathbf{y}) + d(\mathbf{y},\mathbf{z}) \geq d(\mathbf{x},\mathbf{z}).$$

3.8 From the given condition, we see that $\lambda < \lfloor \frac{d_{min}-1}{2} \rfloor$. It follows from the theorem 3.5 that all the error patterns of λ or fewer errors can be used as coset leaders in a standard array. Hence, they are correctable. In order to show that any error pattern of ℓ or fewer errors is detectable, we need to show that no error pattern $\mathbf{x}$ of ℓ or fewer errors can be in the same coset as an error pattern $\mathbf{y}$ of λ or fewer errors. Suppose that $\mathbf{x}$ and $\mathbf{y}$ are in the same coset. Then $\mathbf{x}+\mathbf{y}$ is a nonzero code word. The weight of this code word is

$$w(\mathbf{x}+\mathbf{y}) \leq w(\mathbf{x}) + w(\mathbf{y}) \leq \ell + \lambda < d_{min}.$$

This is impossible since the minimum weight of the code is d_{min}. Hence $\mathbf{x}$ and $\mathbf{y}$ are in different cosets. As a result, when $\mathbf{x}$ occurs, it will not be mistaken as $\mathbf{y}$. Therefore $\mathbf{x}$ is detectable.

3.11 In a systematic linear code, every nonzero code vector has at least one nonzero component in its information section (i.e. the rightmost k positions). Hence a nonzero vector that consists of only zeros in its rightmost k position can not be a code word in any of the systematic code in Γ.

Now consider a nonzero vector $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ with at least one nonzero component in its k rightmost positions,say $v_{n-k+i} = 1$ for $0 \leq i < k$. Consider a matrix of the following form which has $\mathbf{v}$ as its i-th row:

$$\begin{bmatrix} p_{00} & p_{01} & \cdots & p_{0,n-k-1} & 1 & 0 & 0 & 0 & \cdots & 0 \\ p_{10} & p_{11} & \cdots & p_{1,n-k-1} & 0 & 1 & 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots & & & & & & \\ v_0 & v_1 & \cdots & v_{n-k-1} & v_{n-k} & v_{n-k+1} & \cdot & \cdot & \cdots & v_{n-1} \\ p_{i+1,0} & p_{i+1,1} & \cdots & p_{i+1,n-k-1} & 0 & 0 & \cdot & \cdot & 1 \cdot \cdot & 0 \\ \vdots & & & \vdots & & & & & & \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

By elementary row operations, we can put $\mathbf{G}$ into systematic form $\mathbf{G}_1$. The code generated by $\mathbf{G}_1$ contains $\mathbf{v}$ as a code word. Since each p_{ij} has 2 choices, 0 or 1, there are $2^{(k-1)(n-k)}$ matrices $\mathbf{G}$ with $\mathbf{v}$ as the i-th row. Each can be put into systematic form $\mathbf{G}_1$ and each $\mathbf{G}_1$ generates a systematic code containing $\mathbf{v}$ as a code word. Hence $\mathbf{v}$ is contained in $2^{(k-1)(n-k)}$ codes in Γ.

3.13 The generator matrix of the code is

$$\begin{aligned} \mathbf{G} &= [\mathbf{P}_1 \quad \mathbf{I}_k \quad \mathbf{P}_2 \quad \mathbf{I}_k] \\ &= [\mathbf{G}_1 \quad \mathbf{G}_2] \end{aligned}$$

Hence a nonzero codeword in C is simply a cascade of a nonzero codeword $\mathbf{v}_1$ in C_1 and a nonzero codeword $\mathbf{v}_2$ in C_2, i.e.,

$$(\mathbf{v}_1, \mathbf{v}_2).$$

Since $w(\mathbf{v}_1) \geq d_1$ and $w(\mathbf{v}_2) \geq d_2$, hence $w[(\mathbf{v}_1, \mathbf{v}_2)] \geq d_1 + d_2$.

3.15 It follows from Theorem 3.5 that all the vectors of weight t or less can be used as coset leaders. There are

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$$

such vectors. Since there are 2^{n-k} cosets, we must have

$$2^{n-k} \geq \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}.$$

Taking logarithm on both sides of the above inequality, we obtain the Hamming bound on t,

$$n - k \geq log_2\{1 + \binom{n}{1} + \cdots + \binom{n}{t}\}.$$

3.16 Arrange the 2^k code words as a $2^k \times n$ array. From problem 6(b), each column of this code array contains 2^{k-1} zeros and 2^{k-1} ones. Thus the total number of ones in the array is $n \cdot 2^{k-1}$. Note that each nonzero code word has weight (ones) at least d_{min}. Hence

$$(2^k - 1) \cdot d_{min} \leq n \cdot 2^{k-1}$$

This implies that

$$d_{min} \leq \frac{n \cdot 2^{k-1}}{2^k - 1}.$$

3.17 The number of nonzero vectors of length n and weight $d - 1$ or less is

$$\sum_{i=1}^{d-1} \binom{n}{i}$$

From the result of problem 3.11, each of these vectors is contained in at most $2^{(k-1)(n-k)}$ linear systematic codes. Therefore there are at most

$$M = 2^{(k-1)(n-k)} \sum_{i=1}^{d-1} \binom{n}{i}$$

linear systematic codes contain nonzero codewords of weight $d - 1$ or less. The total number of linear systematic codes is

$$N = 2^{(k(n-k)}$$

If $M < N$, there exists at least one code with minimum weight at least d. $M < N$ implies that

$$2^{(k-1)(n-k)} \sum_{i=1}^{d-1} \binom{n}{i} < 2^{k(n-k)}$$

$$\sum_{i=1}^{d-1} \binom{n}{i} < 2^{(n-k)}.$$

3.18 Let d_{min} be the smallest positive integer such that

$$\sum_{i=1}^{d_{min}-1} \binom{n}{i} < 2^{(n-k)} \leq \sum_{i=1}^{d_{min}} \binom{n}{i}$$

From problem 3.17, the first inequality garantees the existence of a systematic linear code with minimum distance d_{min}.

Chapter 4

4.1 A parity-check matrix for the $(15,11)$ Hamming code is

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Let $\boldsymbol{r} = (r_0, r_1, \ldots, r_{14})$ be the received vector. The syndrome of $\boldsymbol{r}$ is (s_0, s_1, s_2, s_3) with

$$\begin{aligned} s_0 &= r_0 + r_4 + r_7 + r_8 + r_{10} + r_{12} + r_{13} + r_{14}, \\ s_1 &= r_1 + r_4 + r_5 + r_9 + r_{10} + r_{11} + r_{13} + r_{14}, \\ s_2 &= r_2 + r_5 + r_6 + r_8 + r_{10} + r_{11} + r_{12} + r_{14}, \\ s_3 &= r_3 + r_6 + r_7 + r_9 + r_{11} + r_{12} + r_{13} + r_{14}. \end{aligned}$$

Set up the decoding table as Table 4.1. From the decoding table, we find that

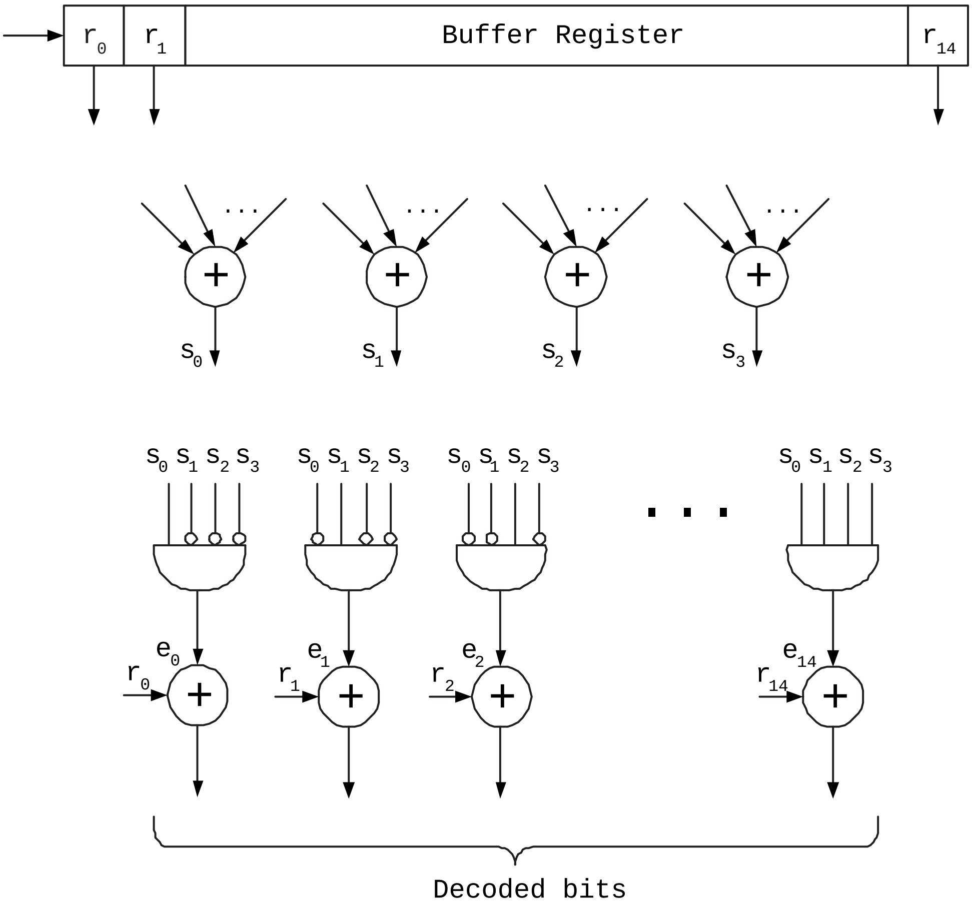
$$e_0 = s_0\bar{s}_1\bar{s}_2\bar{s}_3,\ e_1 = \bar{s}_0 s_1\bar{s}_2\bar{s}_3,\ e_2 = \bar{s}_0\bar{s}_1 s_2\bar{s}_3,$$

$$e_3 = \bar{s}_0\bar{s}_1\bar{s}_2 s_3,\ e_4 = s_0 s_1\bar{s}_2\bar{s}_3,\ e_5 = \bar{s}_0 s_1 s_2\bar{s}_3,$$

$$\ldots,\ e_{13} = s_0 s_1\bar{s}_2 s_3,\ e_{14} = s_0 s_1 s_2 s_3.$$

Table 4.1: Decoding Table

s_0	s_1	s_2	s_3	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
1	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1



4.3 From (4.3), the probability of an undetected error for a Hamming code is

$$P_u(E) = 2^{-m}\{1 + (2^m - 1)(1 - 2p)^{2^{m-1}}\} - (1 - p)^{2^m - 1}$$

$$= 2^{-m} + (1 - 2^{-m})(1 - 2p)^{2^{m-1}} - (1 - p)^{2^m - 1}. \tag{1}$$

Note that

$$(1 - p)^2 \geq 1 - 2p, \tag{2}$$

and

$$(1 - 2^{-m}) \geq 0. \tag{3}$$

Using (2) and (3) in (1), we obtain the following inequality:

$$P_u(E) \leq 2^{-m} + (1 - 2^{-m}) \left[(1 - p)^2\right]^{2^{m-1}} - (1 - p)^{2^m - 1}$$

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

$$= 2^{-m} - (1 - p)^{2^m - 1}\{(1 - (1 - p)(1 - 2^{-m})\}. \tag{4}$$

Note that $0 \leq 1 - p \leq 1$ and $0 \leq 1 - 2^{-m} < 1$. Clearly $0 \leq (1 - p) \cdot (1 - 2^{-m}) < 1$, and

$$1 - (1 - p) \cdot (1 - 2^{-m}) \geq 0. \tag{5}$$

Since $(1 - p)^{2^m - 1} \geq 0$, it follows from (4) and (5) that $P_u(E) \leq 2^{-m}$.

4.6 The generator matrix for the 1st-order RM code RM(1,3) is

$$\mathbf{G} = \begin{bmatrix} \mathbf{v}_0 \\ \mathbf{v}_3 \\ \mathbf{v}_2 \\ \mathbf{v}_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{1}$$

The code generated by this matrix is a $(8, 4)$ code with minimum distance 4. Let (a_0, a_3, a_2, a_1)

be the message to be encoded. Then its corresponding codeword is

$$\mathbf{b} = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)$$

$$= a_0\mathbf{v}_0 + a_3\mathbf{v}_3 + a_2\mathbf{v}_2 + a_1\mathbf{v}_1. \tag{2}$$

From (1) and (2), we find that

$$b_0 = a_0, b_1 = a_0 + a_1, b_2 = a_0 + a_2, b_3 = a_0 + a_2 + a_1,$$

$$b_4 = a_0 + a_3, b_5 = a_0 + a_3 + a_1, b_6 = a_0 + a_3 + a_2,$$

$$b_7 = a_0 + a_3 + a_2 + a_1. \tag{3}$$

From (3), we find that

$$a_1 = b_0 + b_1 = b_2 + b_3 = b_4 + b_5 = b_6 + b_7,$$

$$a_2 = b_0 + b_2 = b_1 + b_3 = b_4 + b_6 = b_5 + b_7,$$

$$a_3 = b_0 + b_4 = b_1 + b_5 = b_2 + b_6 = b_3 + b_7,$$

$$a_0 = b_0 = b_1 + a_1 = b_2 + a_2 = b_3 + a_2 + a_1 = b_4 + a_3$$

$$= b_5 + a_3 + a_1 = b_6 + a_3 + a_2 = b_7 + a_3 + a_2 + a_1.$$

Let $\mathbf{r} = (r_0, r_1, r_2, r_3, r_4, r_5, r_6, r_7)$ be the received vector. The check-sum for decoding a_1, a_2 and a_3 are:

$$\begin{array}{ccc}
(a_1) & (a_2) & (a_3) \\
A_1^{(0)} = r_0 + r_1 & B_1^{(0)} = r_0 + r_2 & C_1^{(0)} = r_0 + r_4 \\
A_2^{(0)} = r_2 + r_3 & B_2^{(0)} = r_1 + r_3 & C_2^{(0)} = r_1 + r_5 \\
A_3^{(0)} = r_4 + r_5 & B_3^{(0)} = r_4 + r_6 & C_3^{(0)} = r_2 + r_6 \\
A_4^{(0)} = r_6 + r_7 & B_4^{(0)} = r_5 + r_7 & C_4^{(0)} = r_3 + r_7
\end{array}$$

After decoding a_1, a_2 and a_3, we form

$$\begin{aligned}\mathbf{r}^{(1)} &= \mathbf{r} - a_1\mathbf{v}_1 - a_2\mathbf{v}_2 - a_3\mathbf{v}_3 \\ &= (r_0^{(1)}, r_1^{(1)}, r_2^{(1)}, r_3^{(1)}, r_4^{(1)}, r_5^{(1)}, r_6^{(1)}, r_7^{(1)}).\end{aligned}$$

Then a_0 is equal to the value taken by the majority of the bits in $\mathbf{r}^{(1)}$.
For decoding (01000101), the four check-sum for decoding a_1, a_2 and a_3 are:

(1) $A_1^{(0)} = 1$, $A_2^{(0)} = 0$, $A_3^{(0)} = 1$, $A_4^{(0)} = 1$;

(2) $B_1^{(0)} = 0$, $B_2^{(0)} = 1$, $B_3^{(0)} = 0$, $B_4^{(0)} = 0$;

(3) $C_1^{(0)} = 0$, $C_2^{(0)} = 0$, $C_3^{(0)} = 0$, $C_4^{(0)} = 1$.

Based on these check-sums, a_1, a_2 and a_3 are decoded as 1, 0 and 0, respectively.
To decode a_0, we form

$$\begin{aligned}\mathbf{r}^{(1)} &= (01000101) - a_1\mathbf{v}_1 - a_2\mathbf{v}_2 - a_3\mathbf{v}_3 \\ &= (00010000).\end{aligned}$$

From the bits of $\mathbf{r}^{(1)}$, we decode a_0 to 0. Therefore, the decoded message is (0001).

4.14

$$\begin{aligned}RM(1,3) = \{ \; & 0, 1, X_1, X_2, X_3, 1+X_1, 1+X_2, \\ & 1+X_3, X_1+X_2, X_1+X_3, X_2+X_3, \\ & 1+X_1+X_2, 1+X_1+X_3, 1+X_2+X_3, \\ & X_1+X_2+X_3, 1+X_1+X_2+X_3\}.\end{aligned}$$

4.15 The RM$(r, m-1)$ and RM$(r-1, m-1)$ codes are given as follows (from (4.38)):

$$\begin{aligned}RM(r, m-1) &= \{\mathbf{v}(f) : f(X_1, X_2, \ldots, X_{m-1}) \in \mathcal{P}(r, m-1)\}, \\ RM(r-1, m-1) &= \{\mathbf{v}(g) : g(X_1, X_2, \ldots, X_{m-1}) \in \mathcal{P}(r-1, m-1)\}.\end{aligned}$$

Then

$$\text{RM}(r,m)\text{=}\{\mathbf{v}(h) : h = f(X_1, X_2, \ldots, X_{m-1}) + X_m g(X_1, X_2, \ldots, X_{m-1})$$
$$\text{with } f \in \mathcal{P}(r, m-1) \text{ and } g \in \mathcal{P}(r-1, m-1)\}.$$

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,

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

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

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

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.

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

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 $-t \leq i \leq t$, 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).

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

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

7.4 The syndrome components of the received polynomial are:

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

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,

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

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

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

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:

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

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

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 α, $\alpha^2, \ldots, \alpha^{d-1}$ 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 α, $\alpha^2, \ldots, \alpha^{d-1}$ (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 $\{\mathbf{v(X)}\}$ 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).

Chapter 8

8.2 The order of the perfect difference set $\{0, 2, 3\}$ is $q = 2$.

(a) The length of the code $n = 2^2 + 2 + 1 = 7$.

(b) Let $\boldsymbol{z}(X) = 1 + X^2 + X^3$. Then the parity-check polynomial is

$$\boldsymbol{h}(X) = GCD\{1 + X^2 + X^3, X^7 + 1\} = 1 + X^2 + X^3.$$

(c) The generator polynomial is

$$\boldsymbol{g}(X) = \frac{X^7 + 1}{\boldsymbol{h}(X)} = 1 + X^2 + X^3 + X^4.$$

(d) From $\boldsymbol{g}(X)$, we find that the generator matrix in systematic form is

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

The parity-check matrix in systematic form is

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

The check-sums orthogonal on the highest order error digit e_6 are:

$$\begin{aligned} A_1 &= s_0 + s_2, \\ A_2 &= s_1, \\ A_3 &= s_3. \end{aligned}$$

Based on the above check-sum, a type-1 decoder can be implemented.

8.4 (a) Since all the columns of $\mathbf{H}$ are distinct and have odd weights, no two or three columns can sum to zero, hence the minimum weight of the code is at least 4. However, the first, the second, the third and the 6th columns sum to zero. Therefore the minimum weight, hence the minimum distance, of the code is 4.

(b) The syndrome of the error vector $\boldsymbol{e}$ is

$$\boldsymbol{s} = (s_0, s_1, s_2, s_3, s_4) = \boldsymbol{e}\mathbf{H}^T$$

with

$$\begin{aligned} s_0 &= e_0 + e_5 + e_6 + e_7 + e_8 + e_9 + e_{10}, \\ s_1 &= e_1 + e_5 + e_6 + e_8, \\ s_2 &= e_2 + e_5 + e_7 + e_9, \\ s_3 &= e_3 + e_6 + e_7 + e_{10}, \\ s_4 &= e_4 + e_8 + e_9 + e_{10}. \end{aligned}$$

(c) The check-sums orthogonal on e_{10} are:

$$\begin{aligned} A_{1,10} &= s_0 + s_1 + s_2 = e_0 + e_1 + e_2 + e_5 + e_{10}, \\ A_{2,10} &= s_3 = e_3 + e_6 + e_7 + e_{10}, \\ A_{3,10} &= s_4 = e_4 + e_8 + e_9 + e_{10}. \end{aligned}$$

The check-sums orthogonal on e_9 are:

$$\begin{aligned} A_{1,9} &= s_0 + s_1 + s_3, \\ A_{2,9} &= s_2, \\ A_{3,9} &= s_4. \end{aligned}$$

The check-sums orthogonal on e_8 are:

$$\begin{aligned} A_{1,8} &= s_0 + s_2 + s_3, \\ A_{2,8} &= s_1, \\ A_{3,8} &= s_4. \end{aligned}$$

The check-sums orthogonal on e_7 are:

$$\begin{aligned} A_{1,7} &= s_0 + s_1 + s_4, \\ A_{2,7} &= s_2, \\ A_{3,7} &= s_3. \end{aligned}$$

The check-sums orthogonal on e_6 are:

$$\begin{aligned} A_{1,6} &= s_0 + s_2 + s_4, \\ A_{2,6} &= s_1, \\ A_{3,6} &= s_3. \end{aligned}$$

The check-sums orthogonal on e_5 are:

$$\begin{aligned} A_{1,5} &= s_0 + s_3 + s_4, \\ A_{2,5} &= s_1, \\ A_{3,5} &= s_2. \end{aligned}$$

(d) Yes, the code is completely orthogonalizable, since there are 3 check-sums orthogonal on each message bit and the minimum distance of the code is 4.

8.5 For $m = 6$, the binary radix-2 form of 43 is

$$43 = 1 + 2 + 2^3 + 2^5.$$

The nonzero-proper descendants of 43 are:

$$1, 2, 8, 32, 3, 9, 33, 10, 34, 40, 11, 35, 41, 42.$$

8.6

$$\begin{array}{ccccccccccccccccccc} & & & \alpha^\infty & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & \\ \boldsymbol{u} & = & (& 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 &) \end{array}$$

Applying the permutation $Z = \alpha^3 Y + \alpha^{11}$ to the above vector, the component at the location α^i is permute to the location $\alpha^3\alpha^i + \alpha^{11}$. For example, the 1-component at the location $Y = \alpha^8$ is permuted to the location $\alpha^3\alpha^8 + \alpha^{11} = \alpha^{11} + \alpha^{11} = \alpha^\infty$. Performing this permutation to the each component of the above vector, we obtain the following vector

$$\begin{array}{ccccccccccccccccccc} & & & \alpha^{\infty} & \alpha^{0} & \alpha^{1} & \alpha^{2} & \alpha^{3} & \alpha^{4} & \alpha^{5} & \alpha^{6} & \alpha^{7} & \alpha^{8} & \alpha^{9} & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & \\ \boldsymbol{v} & = & (& 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 &) \end{array}$$

8.7 For $J = 9$ and $L = 7$, $X^{63} + 1$ can be factor as follows:

$$X^{63} + 1 = (1 + X^9)(1 + X^9 + X^{18} + X^{27} + X^{36} + X^{45} + X^{54}).$$

Then $\pi(X) = 1+X^9+X^{18}+X^{27}+X^{36}+X^{45}+X^{54}$. Let α be a primitive element in GF(2^6) whose minimal polynomial is $\phi_1(X) = 1+X+X^6$. Because $\alpha^{63} = 1$, the polynomial $1+X^9$ has α^0, α^7, α^{14}, α^{21}, α^{28}, α^{35}, α^{42}, α^{49}, and α^{56} as all it roots. Therefore, the polynomial $\pi(X)$ has α^h as a root when h is not a multiple of 7 and $0 < h < 63$. From the conditions (Theorem 8.2) on the roots of $H(X)$, we can find $H(X)$ as: $H(X)$ = LCM$\{$minimal polynomials $\phi_i(X)$ of the roots of $H(X)\}$. As the result,

$$H(X) = \phi_1(X)\phi_3(X)\phi_5(X)\phi_9(X)\phi_{11}(X)\phi_{13}(X)\phi_{27}(X),$$

where $\phi_1 = 1 + X + X^6$, $\phi_3 = 1 + X + X^2 + X^4 + X^6$, $\phi_5 = 1 + X + X^2 + X^5 + X^6$, $\phi_9 = 1 + X^2 + X^3$, $\phi_{11} = 1 + X^2 + X^3 + X^5 + X^6$, $\phi_{13} = 1 + X + X^3 + X^4 + X^6$, and $\phi_{27} = 1 + X + X^3$. Then, we can find $G(X)$,

$$\begin{aligned} G(X) &= \frac{X^{63}+1}{H(X)} = \frac{(1+X^9)\pi(X)}{H(X)} \\ &= (1+X^9)(1+X^2+X^4+X^5+X^6)(1+X+X^4+X^5+X^6)(1+X^5+X^6). \end{aligned}$$

For type-1 DTI code of length 63 and $J = 9$, the generator polynomial is:

$$\begin{aligned} \boldsymbol{g}_1(X) &= \frac{X^{27}G(X^{-1})}{1+X} = \frac{(1+X^9)(1+X+X^2+X^4+X^6)(1+X+X^2+X^5+X^6)(1+X+X^6)}{1+X} \\ &= (1+X+X^2+X^3+X^4+X^5+X^6+X^7+X^8)(1+X+X^2+X^4+X^6) \\ &\quad (1+X+X^2+X^5+X^6)(1+X+X^6). \end{aligned}$$

Represent the polynomials $\pi(X)$, $X\pi(X)$, $X^2\pi(X)$, $X^3\pi(X)$, $X^4\pi(X)$, $X^5\pi(X)$, $X^6\pi(X)$, $X^7\pi(X)$, and $X^8\pi(X)$ by 63-tuple location vectors. Add an overall parity-check digit and apply the affine permutation, $Y = \alpha X + \alpha^{62}$, to each of these location vectors. Then, remove the overall parity-check digits of all location vectors. By removing one vector with odd weight, we can obtain the polynomials orthogonal on the digit position X^{62}. They are:

$$X^{11} + X^{16} + X^{18} + X^{24} + X^{48} + X^{58} + X^{59} + X^{62},$$

$$X^{1} + X^{7} + X^{31} + X^{41} + X^{42} + X^{45} + X^{57} + X^{62},$$

$$X^{23} + X^{33} + X^{34} + X^{37} + X^{49} + X^{54} + X^{56} + X^{62},$$

$$X^{2} + X^{14} + X^{19} + X^{21} + X^{27} + X^{51} + X^{61} + X^{62},$$

$$X^{0} + X^{3} + X^{15} + X^{20} + X^{22} + X^{28} + X^{52} + X^{62},$$

$$X^{9} + X^{10} + X^{13} + X^{25} + X^{30} + X^{32} + X^{38} + X^{62},$$

$$X^{4} + X^{6} + X^{12} + X^{36} + X^{46} + X^{47} + X^{50} + X^{62},$$

$$X^{5} + X^{29} + X^{39} + X^{40} + X^{43} + X^{55} + X^{60} + X^{62}.$$

8.8 For $J = 7$ and $L = 9$,

$$X^{63} + 1 = (1 + X^7)(1 + X^7 + X^{14} + X^{21} + X^{28} + X^{35} + X^{42} + X^{49} + X^{56})$$

and $\pi(X) = 1+X^7+X^{14}+X^{21}+X^{28}+X^{35}+X^{42}+X^{49}+X^{56}$. Let α be a primitive element in GF(2^6) whose minimal polynomial is $\phi_1(X) = 1+X+X^6$. Because $\alpha^{63} = 1$, the polynomial $1 + X^7$ has α^0, α^9, α^{18}, α^{27}, α^{36}, α^{45}, and α^{54} as all it roots. Therefore, the polynomial $\pi(X)$ has α^h as a root when h is not a multiple of 9 and $0 < h < 63$. From the conditions (Theorem 8.2) on the roots of $H(X)$, we can find $H(X)$ as: $H(X)$ = LCM{minimal polynomials $\phi_i(X)$ of the roots of $H(X)$}. As the result,

$$H(X) = \phi_1(X)\phi_3(X)\phi_5(X)\phi_7(X)\phi_{21}(X),$$

where $\phi_1 = 1 + X + X^6$, $\phi_3 = 1 + X + X^2 + X^4 + X^6$, $\phi_5 = 1 + X + X^2 + X^5 + X^6$, $\phi_7 = 1 + X^3 + X^6$, and $\phi_{21} = 1 + X + X^2$. Then, we can find $G(X)$,

$$\begin{aligned} G(X) &= \frac{X^{63}+1}{H(X)} = \frac{(1+X^7)\pi(X)}{H(X)} \\ &= (1+X^7)(1+X^2+X^3+X^5+X^6)(1+X+X^3+X^4+X^6) \\ &\quad (1+X^2+X^4+X^5+X^6)(1+X+X^4+X^5+X^6)(1+X^5+X^6). \end{aligned}$$

For type-1 DTI code of length 63 and $J = 7$, the generator polynomial is:

$$\begin{aligned}
\boldsymbol{g}_1(X) &= \frac{X^{37}G(X^{-1})}{1+X} \\
&= \frac{(1+X^7)(1+X+X^3+X^4+X^6)(1+X^2+X^3+X^5+X^6)}{1+X} \\
& \quad (1+X+X^2+X^4+X^6)(1+X+X^2+X^5+X^6)(1+X+X^6) \\
&= (1+X+X^2+X^3+X^4+X^5+X^6)(1+X+X^3+X^4+X^6)(1+X^2+X^3+X^5+X^6) \\
& \quad (1+X+X^2+X^4+X^6)(1+X+X^2+X^5+X^6)(1+X+X^6).
\end{aligned}$$

Represent the polynomials $\pi(X)$, $X\pi(X)$, $X^2\pi(X)$, $X^3\pi(X)$, $X^4\pi(X)$, $X^5\pi(X)$, and $X^6\pi(X)$ by 63-tuple location vectors. Add an overall parity-check digit and apply the affine permutation, $Y = \alpha X + \alpha^{62}$, to each of these location vectors. By removing one vector with odd weight, we can obtain the polynomials orthogonal on the digit position X^{62}. They are:

$$X^{11} + X^{14} + X^{32} + X^{36} + X^{43} + X^{44} + X^{45} + X^{52} + X^{56} + X^{62},$$

$$X^{3} + X^{8} + X^{13} + X^{19} + X^{31} + X^{33} + X^{46} + X^{48} + X^{60} + X^{62},$$

$$X^{2} + X^{10} + X^{23} + X^{24} + X^{26} + X^{28} + X^{29} + X^{42} + X^{50} + X^{62},$$

$$X^{1} + X^{6} + X^{9} + X^{15} + X^{16} + X^{35} + X^{54} + X^{55} + X^{61} + X^{62},$$

$$X^{0} + X^{4} + X^{7} + X^{17} + X^{27} + X^{30} + X^{34} + X^{39} + X^{58} + X^{62},$$

$$X^{5} + X^{21} + X^{22} + X^{38} + X^{47} + X^{49} + X^{53} + X^{57} + X^{59} + X^{62}.$$

8.9 The generator polynomial of the maximum-length sequence code of length $n = 2^m - 1$ is

$$\boldsymbol{g}(X) = (X^n + 1)/\boldsymbol{p}(X) = (X+1)(1 + X + X^2 + \ldots + X^{n-1})/\boldsymbol{p}(X),$$

where $\boldsymbol{p}(X)$ is a primitive polynomial of degree m over GF(2). Since $\boldsymbol{p}(X)$ and $(X+1)$ are relatively prime, $\boldsymbol{g}(X)$ has 1 as a root. Since the all-one vector $1 + X + X^2 + \ldots + X^{n-1}$ does not have 1 as a root, it is not divisible by $\boldsymbol{g}(X)$. Therefore, the all-one vector is not a codeword in a maximum-length sequence code.

8.17 There are five 1-flats that pass through the point α^7. The 1-flats passing through α^7 can be represented by $\alpha^7 + \beta a_1$, where a_1 is linearly independent of α^7 and $\beta \in GF(2^2)$. They are five 1-flats passing through α^7 which are:

$$\begin{aligned}
L_1 &= \{\alpha^7, \alpha^9, \alpha^{13}, \alpha^6\}, \\
L_2 &= \{\alpha^7, \alpha^{14}, \alpha^{10}, \alpha^8\}, \\
L_3 &= \{\alpha^7, \alpha^{12}, 0, \alpha^2\}, \\
L_4 &= \{\alpha^7, \alpha^4, \alpha^{11}, \alpha^5\}, \\
L_5 &= \{\alpha^7, \alpha^3, 1, \alpha\}.
\end{aligned}$$

8.18 (a) There are twenty one 1-flats that pass through the point α^{63}. They are:

$$\begin{aligned}
L_1 &= \{\alpha^{63}, 0, \alpha^{42}, \alpha^{21}\} \\
L_2 &= \{\alpha^{63}, \alpha^6, \alpha^{50}, \alpha^{39}\} \\
L_3 &= \{\alpha^{63}, \alpha^{12}, \alpha^{15}, \alpha^{37}\} \\
L_4 &= \{\alpha^{63}, \alpha^{32}, \alpha^4, \alpha^9\} \\
L_5 &= \{\alpha^{63}, \alpha^{24}, \alpha^{11}, \alpha^{30}\} \\
L_6 &= \{\alpha^{63}, \alpha^{62}, \alpha^7, \alpha^{17}\} \\
L_7 &= \{\alpha^{63}, \alpha^1, \alpha^{18}, \alpha^8\} \\
L_8 &= \{\alpha^{63}, \alpha^{26}, \alpha^{41}, \alpha^{38}\} \\
L_9 &= \{\alpha^{63}, \alpha^{48}, \alpha^{60}, \alpha^{22}\} \\
L_{10} &= \{\alpha^{63}, \alpha^{45}, \alpha^{46}, \alpha^{53}\} \\
L_{11} &= \{\alpha^{63}, \alpha^{61}, \alpha^{34}, \alpha^{14}\} \\
L_{12} &= \{\alpha^{63}, \alpha^{25}, \alpha^3, \alpha^{51}\} \\
L_{13} &= \{\alpha^{63}, \alpha^2, \alpha^{16}, \alpha^{36}\} \\
L_{14} &= \{\alpha^{63}, \alpha^{35}, \alpha^{31}, \alpha^{40}\} \\
L_{15} &= \{\alpha^{63}, \alpha^{52}, \alpha^{13}, \alpha^{19}\} \\
L_{16} &= \{\alpha^{63}, \alpha^{23}, \alpha^{54}, \alpha^{58}\} \\
L_{17} &= \{\alpha^{63}, \alpha^{33}, \alpha^{44}, \alpha^{57}\} \\
L_{18} &= \{\alpha^{63}, \alpha^{47}, \alpha^{49}, \alpha^{20}\}
\end{aligned}$$

$$\begin{aligned}
L_{19} &= \{\alpha^{63}, \alpha^{27}, \alpha^{43}, \alpha^{29}\} \\
L_{20} &= \{\alpha^{63}, \alpha^{56}, \alpha^{55}, \alpha^{10}\} \\
L_{21} &= \{\alpha^{63}, \alpha^{59}, \alpha^{28}, \alpha^{5}\}
\end{aligned}$$

(b) There are five 2-flats that intersect on the 1-flat, $\{\alpha^{63} + \eta\alpha\}$, where $\eta \in GF(2^2)$. They are:

$$\begin{aligned}
F_1 &= \{1, \alpha^6, \alpha^{50}, \alpha^{39}, 0, \alpha, \alpha^{22}, \alpha^{43}, \alpha^{42}, \alpha^{29}, \alpha^{18}, \alpha^{48}, \alpha^{21}, \alpha^{60}, \alpha^{27}, \alpha^{8}\} \\
F_2 &= \{1, \alpha^6, \alpha^{50}, \alpha^{39}, \alpha^{12}, \alpha^{26}, \alpha^{10}, \alpha^{46}, \alpha^{15}, \alpha^{53}, \alpha^{41}, \alpha^{56}, \alpha^{37}, \alpha^{55}, \alpha^{45}, \alpha^{38}\} \\
F_3 &= \{1, \alpha^6, \alpha^{50}, \alpha^{39}, \alpha^{32}, \alpha^{35}, \alpha^{20}, \alpha^{57}, \alpha^{4}, \alpha^{33}, \alpha^{31}, \alpha^{47}, \alpha^{9}, \alpha^{49}, \alpha^{44}, \alpha^{40}\} \\
F_4 &= \{1, \alpha^6, \alpha^{50}, \alpha^{39}, \alpha^{24}, \alpha^{16}, \alpha^{34}, \alpha^{17}, \alpha^{11}, \alpha^{62}, \alpha^{36}, \alpha^{14}, \alpha^{30}, \alpha^{61}, \alpha^{7}, \alpha^{2}\} \\
F_5 &= \{1, \alpha^6, \alpha^{50}, \alpha^{39}, \alpha^{25}, \alpha^{5}, \alpha^{54}, \alpha^{52}, \alpha^{3}, \alpha^{13}, \alpha^{59}, \alpha^{58}, \alpha^{51}, \alpha^{23}, \alpha^{19}, \alpha^{28}\}
\end{aligned}$$

8.19 The 1-flats that pass through the point α^{21} are:

$$\begin{aligned}
L_1 &= \{\alpha^{21}, \alpha^{42}, \alpha^{11}, \alpha^{50}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{37}\} \\
L_2 &= \{\alpha^{21}, \alpha^{60}, \alpha^{35}, \alpha^{31}, \alpha^{47}, \alpha^{54}, \alpha^{32}, \alpha^{52}\} \\
L_3 &= \{\alpha^{21}, \alpha^{58}, \alpha^{9}, \alpha^{26}, \alpha^{6}, \alpha^{5}, \alpha^{28}, \alpha^{34}\} \\
L_4 &= \{\alpha^{21}, \alpha^{30}, \alpha^{57}, 0, \alpha^{3}, \alpha^{48}, \alpha^{39}, \alpha^{12}\} \\
L_5 &= \{\alpha^{21}, \alpha^{51}, \alpha^{61}, \alpha^{27}, \alpha^{19}, \alpha^{14}, \alpha^{62}, \alpha^{2}\} \\
L_6 &= \{\alpha^{21}, \alpha^{38}, \alpha^{40}, \alpha^{33}, \alpha^{46}, \alpha^{17}, \alpha^{18}, \alpha^{7}\} \\
L_7 &= \{\alpha^{21}, \alpha^{29}, \alpha^{16}, \alpha^{53}, \alpha^{23}, \alpha^{0}, \alpha^{4}, \alpha^{1}\} \\
L_8 &= \{\alpha^{21}, \alpha^{59}, \alpha^{15}, \alpha^{45}, \alpha^{56}, \alpha^{8}, \alpha^{55}, \alpha^{13}\} \\
L_9 &= \{\alpha^{21}, \alpha^{43}, \alpha^{41}, \alpha^{20}, \alpha^{10}, \alpha^{36}, \alpha^{24}, \alpha^{49}\}
\end{aligned}$$

8.20 a. The radix-2^3 expansion of 47 is expressed as follows:

$$47 = 7 + 5 \cdot 2^3.$$

Hence, the 2^3-weight of 47

$$W_{2^3}(47) = 7 + 5 = 12.$$

b.

$$W_{2^3}(47^{(0)}) = W_{2^3}(47) = 7 + 5 = 12,$$

$$W_{2^3}(47^{(1)}) = W_{2^3}(31) = 7 + 3 = 10,$$

$$W_{2^3}(47^{(2)}) = W_{2^3}(62) = 6 + 7 = 13.$$

Hence,

$$\max_{0 \le l < 3} W_{2^3}(47^{(l)}) = 13.$$

c. All the positive integers h less than 63 such that

$$0 < \max_{0 \le l < 3} W_{2^3}(h^{(l)}) \le 2^3 - 1.$$

are

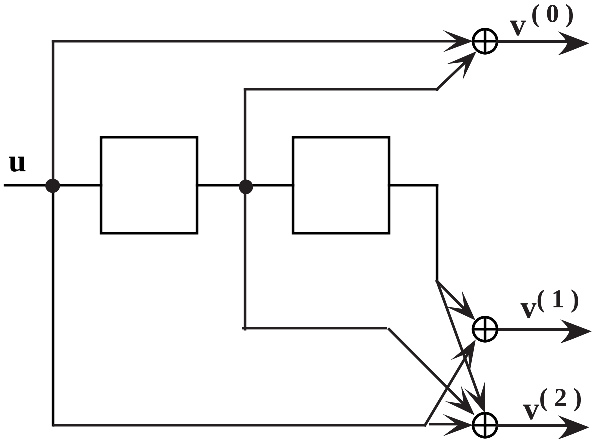
$$1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 17, 20,$$

$$21, 24, 28, 32, 33, 34, 35, 40, 42, 48, 49, 56.$$

Chapter 11

Convolutional Codes

11.1 (a) The encoder diagram is shown below.



(b) The generator matrix is given by

$$\mathbf{G} = \begin{bmatrix} 111 & 101 & 011 & & & \\ & 111 & 101 & 011 & & \\ & & 111 & 101 & 011 & \\ & & & \ddots & & \ddots \end{bmatrix}.$$

(c) The codeword corresponding to $\mathbf{u} = (11101)$ is given by

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G} = (111, 010, 001, 110, 100, 101, 011).$$

11.2 (a) The generator sequences of the convolutional encoder in Figure 11.3 on page 460 are given in (11.21).

(b) The generator matrix is given by

$$\mathbf{G} = \begin{bmatrix} 1111 & 0000 & 0000 & & \\ 0101 & 0110 & 0000 & & \\ 0011 & 0100 & 0011 & & \\ & 1111 & 0000 & 0000 & \\ & 0101 & 0110 & 0000 & \\ & 0011 & 0100 & 0011 & \\ & & \ddots & & \ddots \end{bmatrix}.$$

(c) The codeword corresponding to $\mathbf{u} = (110, 011, 101)$ is given by

$$\mathbf{v} = \mathbf{u} \cdot \mathbf{G} = (1010, 0000, 1110, 0111, 0011).$$

11.3 (a) The generator matrix is given by

$$\mathbf{G}(D) = \left[\begin{array}{ccc} 1+D & 1+D^2 & 1+D+D^2 \end{array}\right].$$

(b) The output sequences corresponding to $\mathbf{u}(D) = 1 + D^2 + D^3 + D^4$ are

$$\begin{aligned} \mathbf{V}(D) &= \left[\mathbf{v}^{(0)}(D), \mathbf{v}^{(1)}(D), \mathbf{v}^{(2)}(D)\right] \\ &= \left[1 + D + D^2 + D^5,\ 1 + D^3 + D^5 + D^6,\ 1 + D + D^4 + D^6\right], \end{aligned}$$

and the corresponding codeword is

$$\begin{aligned} \mathbf{v}(D) &= \mathbf{v}^{(0)}(D^3) + D\mathbf{v}^{(1)}(D^3) + D^2\mathbf{v}^{(2)}(D^3) \\ &= 1 + D + D^2 + D^3 + D^5 + D^6 + D^{10} + D^{14} + D^{15} + D^{16} + D^{19} + D^{20}. \end{aligned}$$

11.4 (a) The generator matrix is given by

$$\mathbf{G}(D) = \begin{bmatrix} 1+D & D & 1+D \\ D & 1 & 1 \end{bmatrix}$$

and the composite generator polynomials are

$$\begin{aligned} \mathbf{g}_1(D) &= \mathbf{g}_1^{(0)}(D^3) + D\mathbf{g}_1^{(1)}(D^3) + D^2\mathbf{g}_1^{(2)}(D^3) \\ &= 1 + D^2 + D^3 + D^4 + D^5 \end{aligned}$$

and

$$\begin{aligned} \mathbf{g}_2(D) &= \mathbf{g}_2^{(0)}(D^3) + D\mathbf{g}_2^{(1)}(D^3) + D^2\mathbf{g}_2^{(2)}(D^3) \\ &= D + D^2 + D^3. \end{aligned}$$

(b) The codeword corresponding to the set of input sequences $\mathbf{U}(D) = \left[1 + D + D^3,\ 1 + D^2 + D^3\right]$ is

$$\begin{aligned} \mathbf{v}(D) &= \mathbf{u}^{(1)}(D^3)\mathbf{g}_1(D) + \mathbf{u}^{(2)}(D^3)\mathbf{g}_2(D) \\ &= 1 + D + D^3 + D^4 + D^6 + D^{10} + D^{13} + D^{14}. \end{aligned}$$

11.5 (a) The generator matrix is given by

$$\mathbf{G} = \left[\begin{array}{cccccccccc} 111 & 001 & 010 & 010 & 001 & 011 & & & & \\ & 111 & 001 & 010 & 010 & 001 & 011 & & & \\ & & 111 & 001 & 010 & 010 & 001 & 011 & & \\ & & & \ddots & & & & & & \ddots \end{array} \right].$$

(b) The parity sequences corresponding to $\mathbf{u} = (1101)$ are given by

$$\begin{aligned} \mathbf{v}^{(1)}(D) &= \mathbf{u}(D) \cdot \mathbf{g}^{(1)}(D) \\ &= (1 + D + D^3)(1 + D^2 + D^3 + D^5) \\ &= 1 + D + D^2 + D^3 + D^4 + D^8, \end{aligned}$$

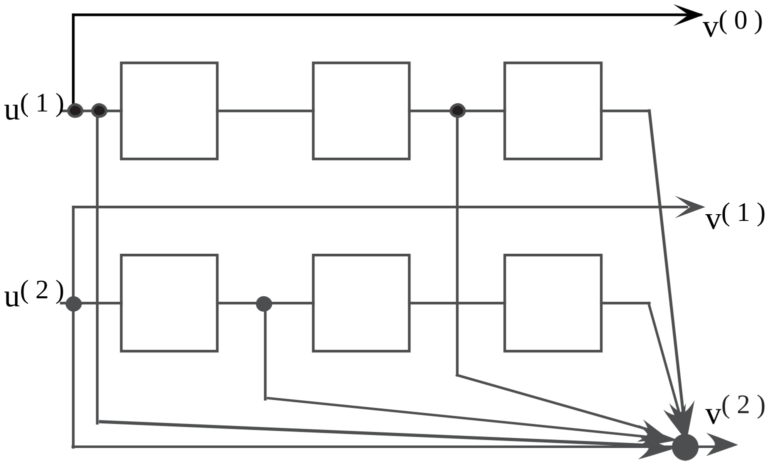
and

$$\begin{aligned} \mathbf{v}^{(2)}(D) &= \mathbf{u}(D) \cdot \mathbf{g}^{(2)}(D) \\ &= (1 + D + D^3)(1 + D + D^4 + D^5) \\ &= 1 + D^2 + D^3 + D^6 + D^7 + D^8. \end{aligned}$$

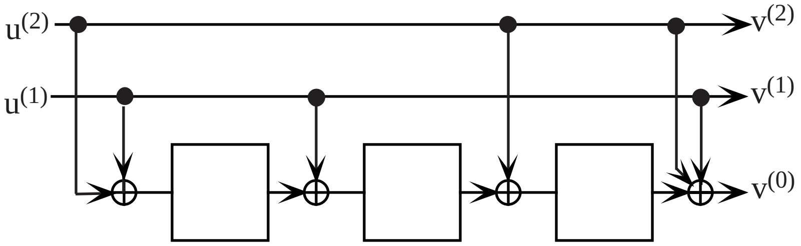
Hence,

$$\begin{aligned} \mathbf{v}^{(1)} &= (111110001) \\ \mathbf{v}^{(2)} &= (101100111). \end{aligned}$$

11.6 (a) The controller canonical form encoder realization, requiring 6 delay elements, is shown below.



(b) The observer canonical form encoder realization, requiring only 3 delay elements, is shown below.



11.14 (a) The GCD of the generator polynomials is 1.

(b) Since the GCD is 1, the inverse transfer function matrix $\mathbf{G}^{-1}(D)$ must satisfy

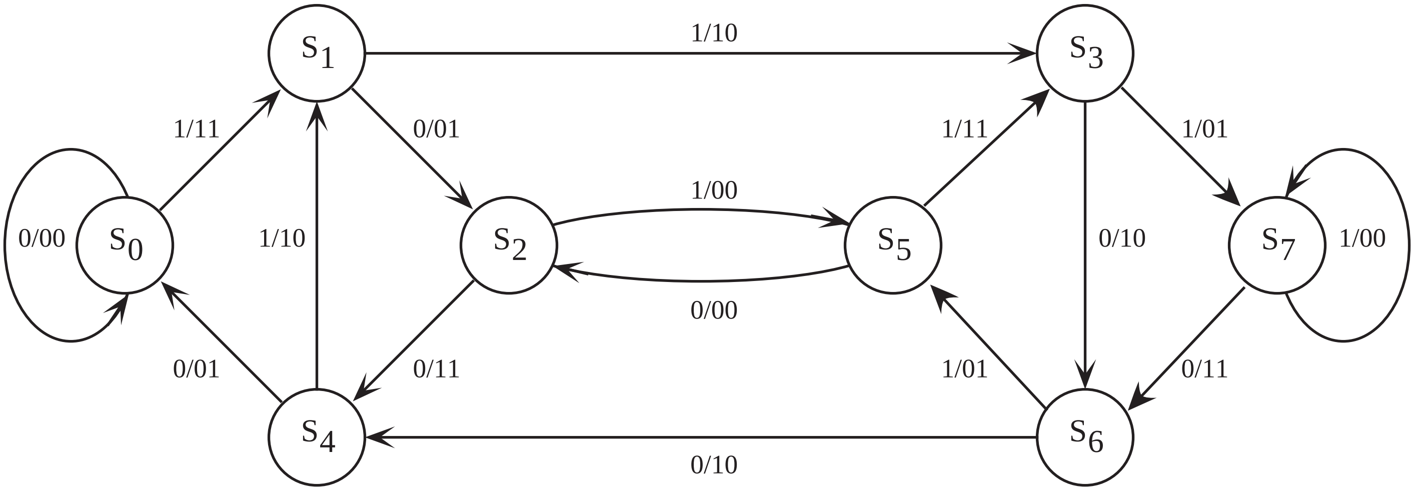
$$\mathbf{G}(D)\mathbf{G}^{-1}(D) = \begin{bmatrix}1+D^2 & 1+D+D^2\end{bmatrix}\mathbf{G}^{-1}(D) = \mathbf{I}.$$

By inspection,

$$\mathbf{G}^{-1}(D) = \begin{bmatrix} 1+D \\ D \end{bmatrix}.$$

11.15 (a) The GCD of the generator polynomials is $1+D^2$ and a feedforward inverse does not exist.

(b) The encoder state diagram is shown below.



(c) The cycles $S_2S_5S_2$ and S_7S_7 both have zero output weight.

(d) The infinite-weight information sequence

$$\mathbf{u}(D) = \frac{1}{1+D^2} = 1 + D^2 + D^4 + D^6 + D^8 + \cdots$$

results in the output sequences

$$\begin{aligned}\mathbf{v}^{(0)}(D) &= \mathbf{u}(D)\left(1+D^2\right) = 1 \\ \mathbf{v}^{(1)}(D) &= \mathbf{u}(D)\left(1+D+D^2+D^3\right) = 1+D,\end{aligned}$$

and hence a codeword of finite weight.

(e) This is a catastrophic encoder realization.

11.16 For a systematic (n, k, ν) encoder, the generator matrix $\mathbf{G}(D)$is a $k \times n$ matrix of the form

$$\mathbf{G}(D) = [\mathbf{I}_k|\mathbf{P}(D)] = \begin{bmatrix} 1 & 0 & \cdots & 0 & \mathbf{g}_1^{(k)}(D) & \cdots & \mathbf{g}_1^{(n-1)}(D) \\ 0 & 1 & \cdots & 0 & \mathbf{g}_2^{(k)}(D) & \cdots & \mathbf{g}_2^{(n-1)}(D) \\ \vdots & & & & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \mathbf{g}_k^{(k)}(D) & \cdots & \mathbf{g}_k^{(n-1)}(D) \end{bmatrix}.$$

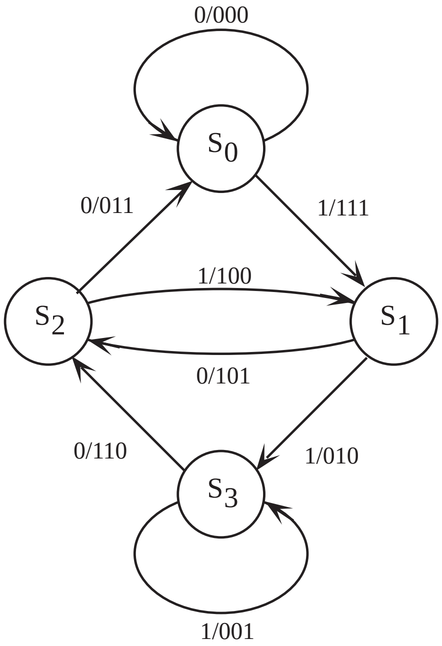
The transfer function matrix of a feedforward inverse $\mathbf{G}^{-1}(D)$ with delay $l = 0$ must be such that

$$\mathbf{G}(D)\mathbf{G}^{-1}(D) = \mathbf{I}_k.$$

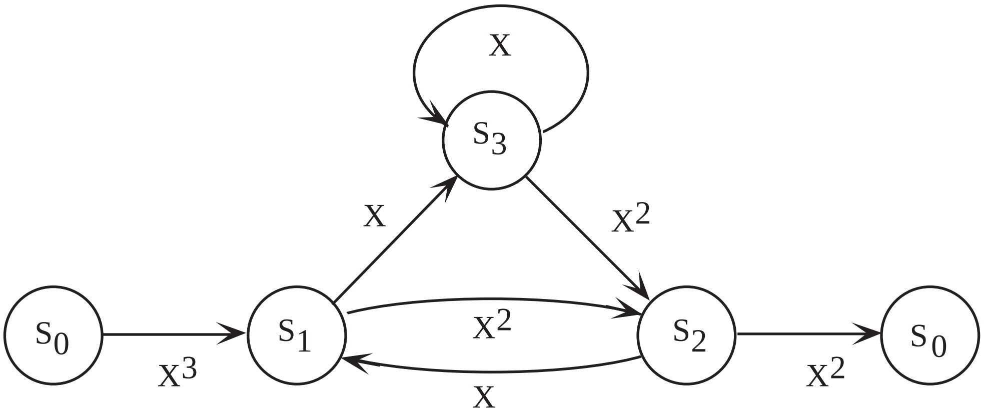
A matrix satisfying this condition is given by

$$\mathbf{G}^{-1}(D) = \begin{bmatrix} \mathbf{I}_k \\ \mathbf{0}_{(n-k)\times k} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}.$$

11.19 (a) The encoder state diagram is shown below.



(b) The modified state diagram is shown below.



(c) The WEF function is given by

$$A(X) = \frac{\sum_i F_i \Delta_i}{\Delta}.$$

There are 3 cycles in the graph:

$$\begin{array}{lll} \text{Cycle 1:} & S_1S_2S_1 & C_1 = X^3 \\ \text{Cycle 2:} & S_1S_3S_2S_1 & C_2 = X^4 \\ \text{Cycle 3:} & S_3S_3 & C_3 = X. \end{array}$$

There is one pair of nontouching cycles:

$$\text{Cycle pair 1:} \quad \text{(Cycle 1, Cycle 3)} \quad C_1C_3 = X^4.$$

There are no more sets of nontouching cycles. Therefore,

$$\begin{aligned} \Delta &= 1 - \sum_i C_i + \sum_{i',j'} C_{i'}C_{j'} \\ &= 1 - (X + X^3 + X^4) + X^4 \\ &= 1 - X - X^3. \end{aligned}$$

There are 2 forward paths:

$$\begin{array}{lll} \text{Forward path 1:} & S_0S_1S_2S_0 & F_1 = X^7 \\ \text{Forward path 2:} & S_0S_1S_3S_2S_0 & F_2 = X^8. \end{array}$$

Only cycle 3 does not touch forward path 1, and hence

$$\Delta_1 = 1 - X.$$

Forward path 2 touches all the cycles, and hence

$$\Delta_2 = 1.$$

Finally, the WEF is given by

$$A(X) = \frac{X^7(1-X) + X^8}{1 - X - X^3} = \frac{X^7}{1 - X - X^3}.$$

Carrying out the division,

$$A(X) = X^7 + X^8 + X^9 + 2X^{10} + \cdots,$$

indicating that there is one codeword of weight 7, one codeword of weight 8, one codeword of weight 9, 2 codewords of weight 10, and so on.

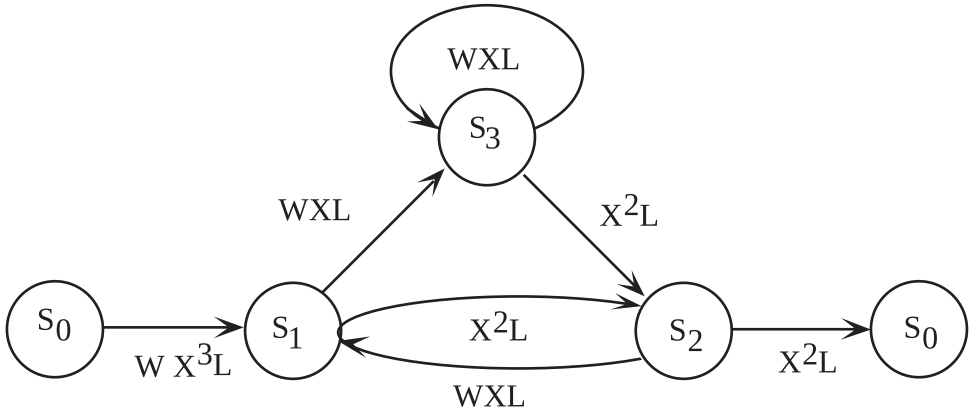
(d) The augmented state diagram is shown below.

(e) The IOWEF is given by

$$A(W, X, L) = \frac{\displaystyle\sum_i F_i \Delta_i}{\Delta}.$$

There are 3 cycles in the graph:

$$\begin{array}{lll} \text{Cycle 1:} & S_1S_2S_1 & C_1 = WX^3L^2 \\ \text{Cycle 2:} & S_1S_3S_2S_1 & C_2 = W^2X^4L^3 \\ \text{Cycle 3:} & S_3S_3 & C_3 = WXL. \end{array}$$



There is one pair of nontouching cycles:

$$\text{Cycle pair 1:} \quad (\text{Cycle 1, Cycle 3}) \quad C_1C_3 = W^2X^4L^3.$$

There are no more sets of nontouching cycles. Therefore,

$$\begin{aligned}\Delta &= 1 - \sum_i C_i + \sum_{i',j'} C_{i'}C_{j'} \\ &= 1 - WX^3L^2 + W^2X^4L^3 + WXL + W^2X^4L^3.\end{aligned}$$

There are 2 forward paths:

$$\begin{array}{lll}\text{Forward path 1:} & S_0S_1S_2S_0 & F_1 = WX^7L^3 \\ \text{Forward path 2:} & S_0S_1S_3S_2S_0 & F_2 = W^2X^8L^4.\end{array}$$

Only cycle 3 does not touch forward path 1, and hence

$$\Delta_1 = 1 - WXL.$$

Forward path 2 touches all the cycles, and hence

$$\Delta_2 = 1.$$

Finally, the IOWEF is given by

$$A(W,X,L) = \frac{WX^7L^3(1-WXL) + W^2X^8L^4}{1-(WX^3L^2 + W^2X^4L^3 + WXL) + X^4Y^2Z^3} = \frac{WX^7L^3}{1-WXL-WX^3L^2}.$$

Carrying out the division,

$$A(W,X,L) = WX^7L^3 + W^2X^8L^4 + W^3X^9L^5 + \cdots,$$

indicating that there is one codeword of weight 7 with an information weight of 1 and length 3, one codeword of weight 8 with an information weight of 2 and length 4, and one codeword of weight 9 with an information weight of 3 and length 5.

11.20 Using state variable method described on pp. 505-506, the WEF is given by

$$A(X)=\frac{-X^4(-1-2X^4+X^3+9X^{20}-42X^{18}+78X^{16}+38X^{12}+3X^{17}+5X^{13}+9X^{11}-9X^{15}-2X^7-74X^{14}-14X^{10}-9X^9+X^6+6X^8)}{1-X+2X^4-X^3-X^2+3X^{24}+X^{21}-3X^{20}+32X^{18}-8X^{22}-X^{19}-45X^{16}-8X^{12}-5X^{17}-6X^{11}+9X^{15}+2X^7+27X^{14}+3X^{10}-2X^9-4X^6+X^8}.$$

Performing the division results in

$$A(X) = X^4 + X^5 + 2X^6 + 3X^7 + 6X^8 + 9X^9 + \cdots,$$

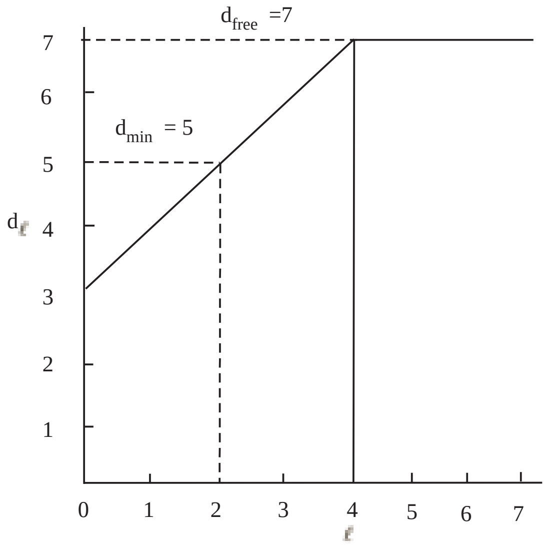
which indicates that there is one codeword of weight 4, one codeword of weight 5, two codewords of weight 6, and so on.

11.28 (a) From Problem 11.19(c), the WEF of the code is

$$A(X) = X^7 + X^8 + X^9 + 2X^{10} + \cdots,$$

and the free distance of the code is therefore $d_{free} = 7$, the lowest power of X in $A(X)$.

(b) The complete CDF is shown below.

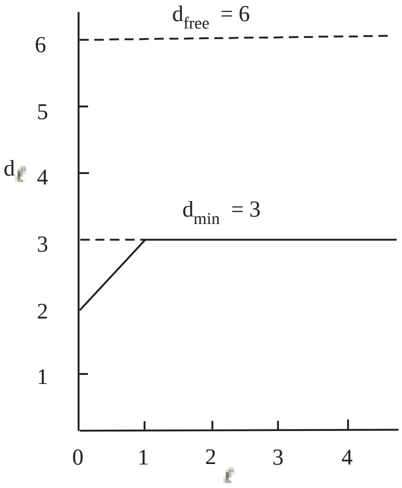


(c) The minimum distance is

$$d_{min} = d_l|_{l=m=2} = 5.$$

11.29 (a) By examining the encoder state diagram in Problem 11.15 and considering only paths that begin *and end* in state S_0 (see page 507), we find that the free distance of the code is $d_{free} = 6$. This corresponds to the path $S_0S_1S_2S_4S_0$ and the input sequence $\mathbf{u} = (1000)$.

(b) The complete CDF is shown below.



(c) The minimum distance is

$$d_{min} = d_l|_{l=m=3} = 3.$$

11.31 By definition, the free distance d_{free} is the minimum weight path that has diverged from and remerged with the all-zero state. Assume that $[\mathbf{v}]_j$ represents the shortest remerged path through the state diagram with weight free d_{free}. Letting $[d_l]_{re}$ be the minimum weight of all remerged paths of length l, it follows that $[d_l]_{re} = d_{free}$ for all $l \geq j$. Also, for a noncatastrophic encoder, any path that remains unmerged must accumulate weight. Letting $[d_l]_{un}$ be the minimum weight of all unmerged paths of length l, it follows that

$$\lim_{l\to\infty} [d_l]_{un} \to \infty.$$

Therefore

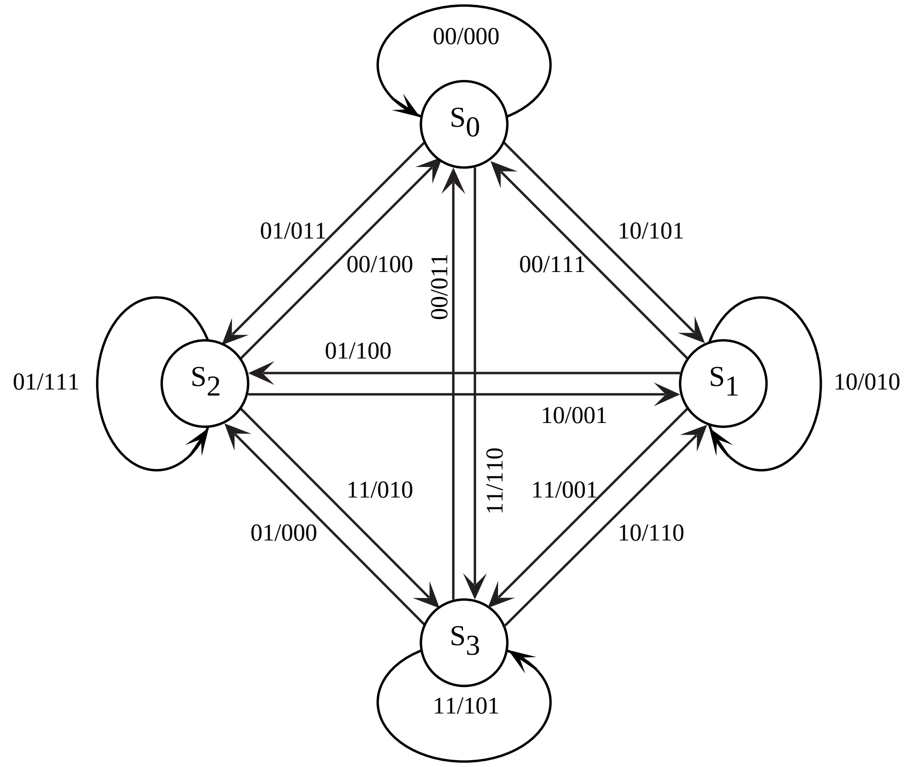
$$\lim_{l\to\infty} d_l = min\left\{\lim_{l\to\infty} [d_l]_{re}, \lim_{l\to\infty} [d_l]_{un}\right\} = d_{free}.$$

Q. E. D.

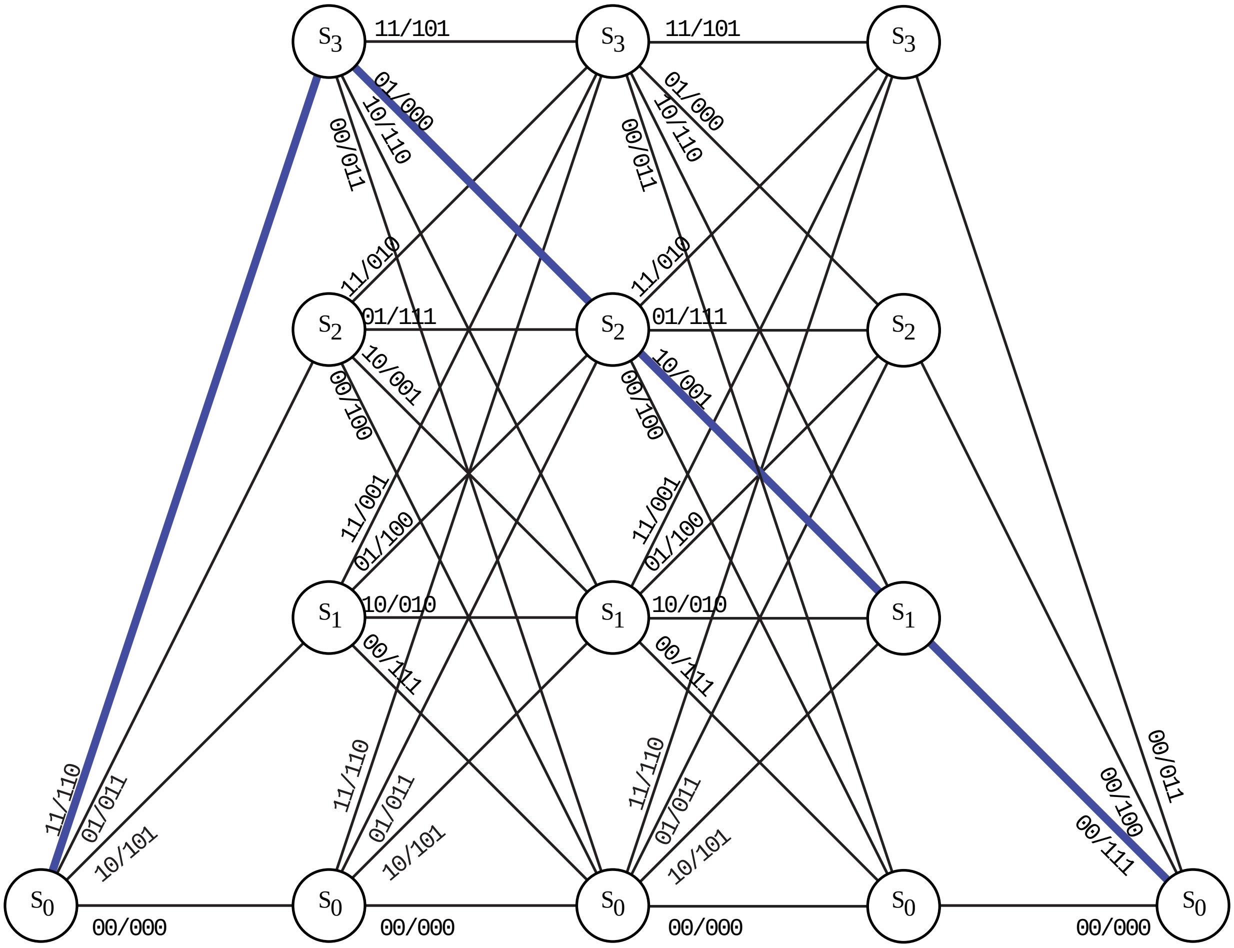
Chapter 12

Optimum Decoding of Convolutional Codes

12.1 (Note: The problem should read “ for the (3,2,2) encoder in Example 11.2 ”rather than “ for the (3,2,2) code in Table 12.1(d)”.) The state diagram of the encoder is given by:



From the state diagram, we can draw a trellis diagram containing $h + m + 1 = 3 + 1 + 1 = 5$ levels as shown below:



Hence, for $\mathbf{u} = (11, 01, 10)$,

$$\begin{aligned} \mathbf{v}^{(0)} &= (1001) \\ \mathbf{v}^{(1)} &= (1001) \\ \mathbf{v}^{(2)} &= (0011) \end{aligned}$$

and

$$\mathbf{v} = (110, 000, 001, 111),$$

agreeing with (11.16) in Example 11.2. The path through the trellis corresponding to this codeword is shown highlighted in the figure.

12.2 Note that

$$\begin{aligned}\sum_{l=0}^{N-1} c_2\left[\log P(r_l|v_l)+c_1\right] &= \sum_{l=0}^{N-1}\left[c_2\log P(r_l|v_l)+c_2c_1\right]\\ &= c_2\sum_{l=0}^{N-1}\log P(r_l|v_l)+Nc_2c_1.\end{aligned}$$

Since

$$\max_{\mathbf{v}}\left\{c_2\sum_{l=0}^{N-1}\log P(r_l|v_l)+Nc_2c_1\right\}=c_2\max_{\mathbf{v}}\left\{\sum_{l=0}^{N-1}\log P(r_l|v_l)\right\}+Nc_2c_1$$

if C_2 is positive, any path that maximizes $\sum_{l=0}^{N-1}\log P(r_l|v_l)$ also maximizes $\sum_{l=0}^{N-1}c_2[\log P(r_l|v_l)+c_1]$.

12.3 The integer metric table becomes:

	0_1	0_2	1_2	1_1
0	6	5	3	0
1	0	3	5	6

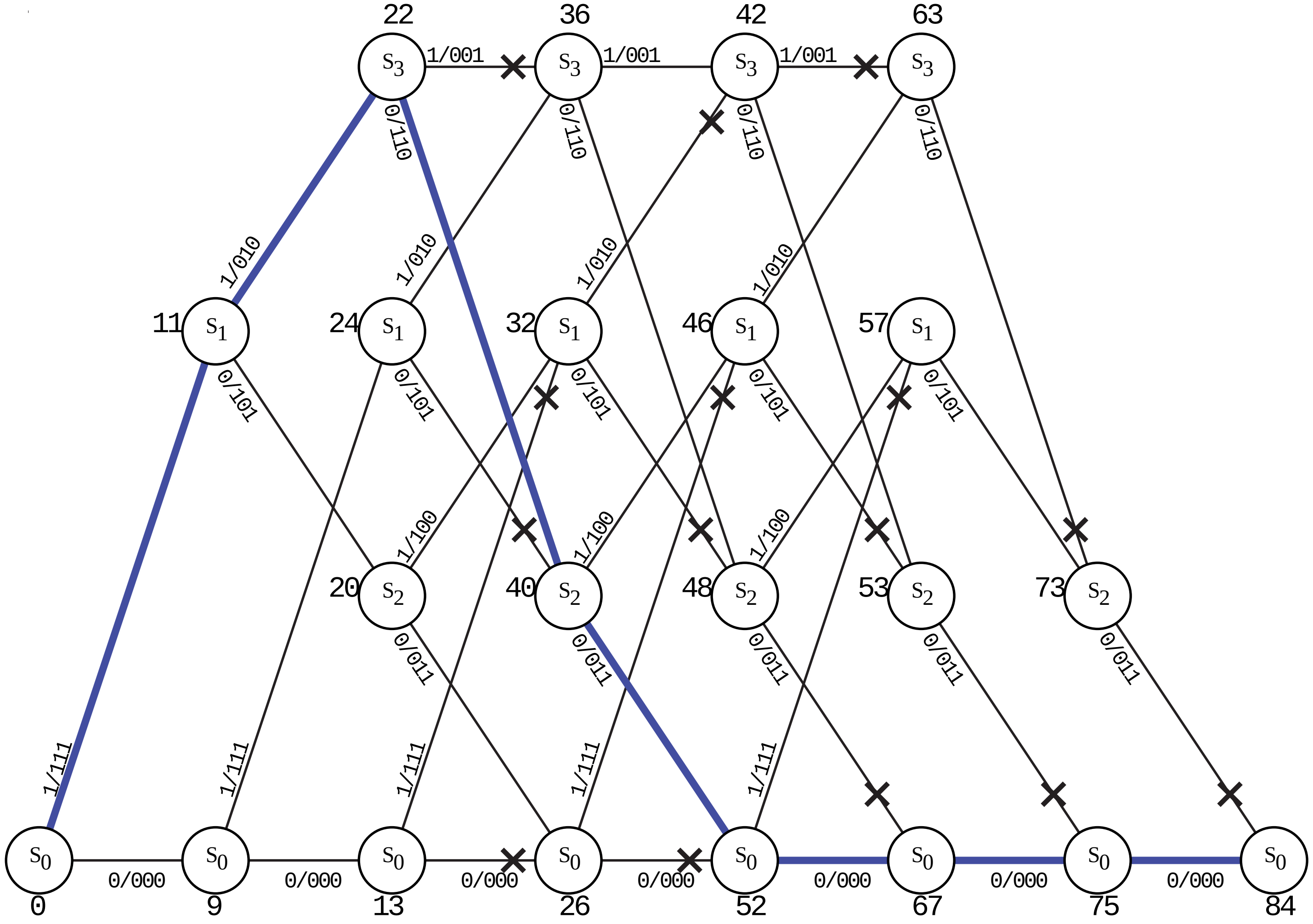
The received sequence is $\mathbf{r}=(1_11_20_1, 1_11_10_2, 1_11_10_1, 1_11_11_1, 0_11_20_1, 1_20_21_1, 1_20_11_1)$. The decoded sequence is shown in the figure below, and the final survivor is

$$\hat{\mathbf{v}}=(111, 010, 110, 011, 000, 000, 000),$$

which yields a decoded information sequence of

$$\hat{\mathbf{u}}=(11000).$$

This result agrees with Example 12.1.


22
36
42
63
S_3
S_3
S_3
S_3
1/001
1/001
1/001
0/110
0/110
0/110
0/110
1/010
1/010
1/010
1/010
11
24
32
46
57
S_1
S_1
S_1
S_1
S_1
0/101
0/101
0/101
0/101
0/101
1/100
1/100
1/100
1/100
20
40
48
53
73
S_2
S_2
S_2
S_2
S_2
0/011
0/011
0/011
0/011
0/011
1/111
1/111
1/111
1/111
1/111
S_0
S_0
S_0
S_0
S_0
S_0
S_0
S_0
S_0
0/000
0/000
0/000
0/000
0/000
0/000
0/000
0/000
0
9
13
26
52
67
75
84

12.4 For the given channel transition probabilities, the resulting metric table is:

	0_1	0_2	0_3	0_4	1_4	1_3	1_2	1_1
0	−0.363	−0.706	−0.777	−0.955	−1.237	−1.638	−2.097	−2.699
1	−2.699	−2.097	−1.638	−1.237	−0.955	−0.777	−0.706	−0.363

To construct an integer metric table, choose $c_1 = 2.699$ and $c_2 = 4.28$. Then the integer metric table becomes:

	0_1	0_2	0_3	0_4	1_4	1_3	1_2	1_1
0	10	9	8	7	6	5	3	0
1	0	3	5	6	7	8	9	10

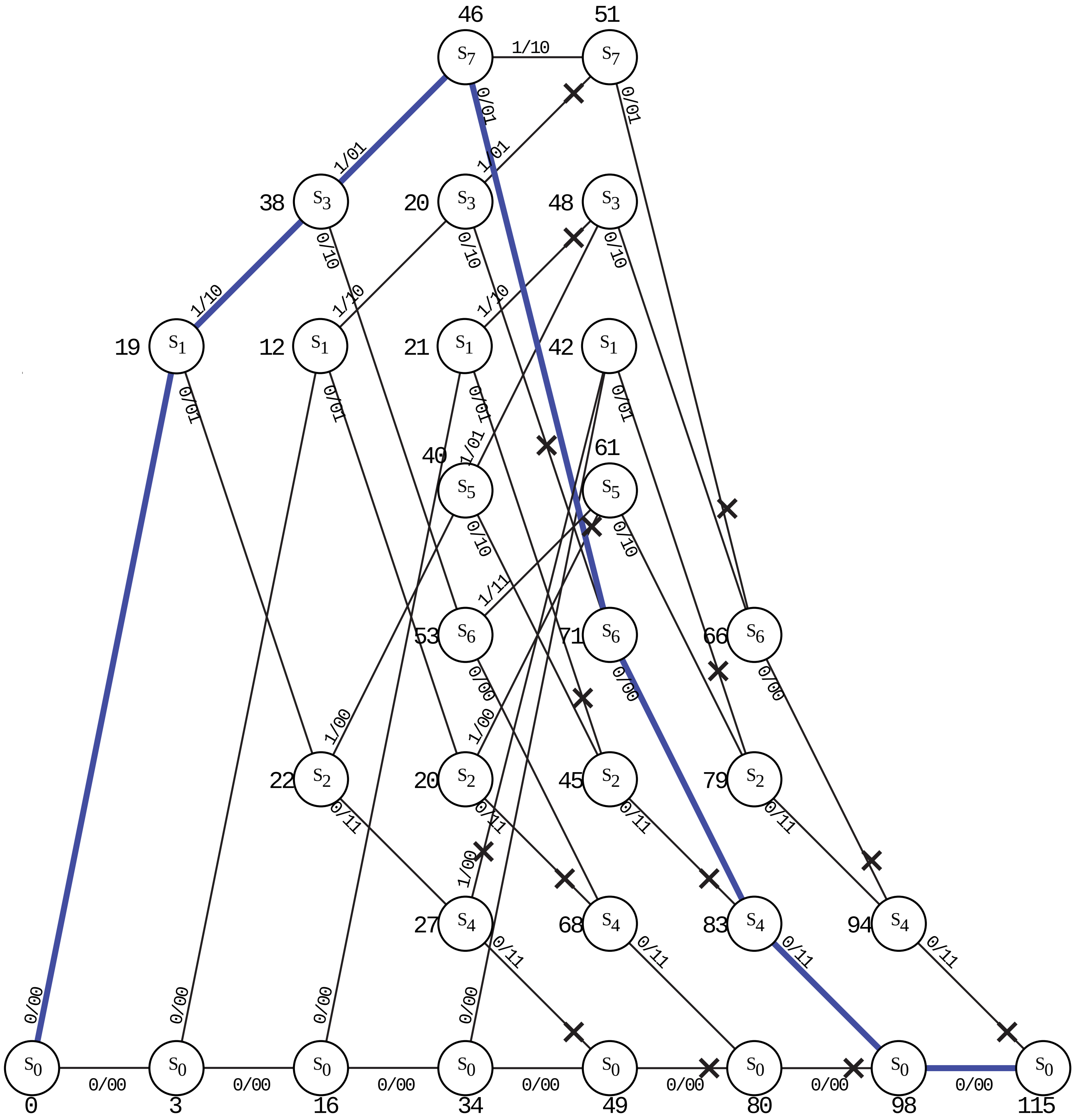
12.5 (a) Referring to the state diagram of Figure 11.13(a), the trellis diagram for an information sequence of length $h = 4$ is shown in the figure below.

(b) After Viterbi decoding the final survivor is

$$\hat{\mathbf{v}} = (11, 10, 01, 00, 11, 00).$$

This corresponds to the information sequence

$$\hat{\mathbf{u}} = (1110).$$


46
51
s7
1/10
s7
0/01
0/01
1/01
1/01
38
s3
20
s3
48
s3
0/10
0/10
0/10
1/10
1/10
1/10
19
s1
12
s1
21
s1
42
s1
0/01
0/01
0/01
0/01
40
1/01
61
s5
s5
0/10
0/10
1/11
53
s6
71
s6
66
s6
0/00
0/00
0/00
1/00
1/00
22
s2
20
s2
45
s2
79
s2
0/11
0/11
0/11
0/11
1/00
27
s4
68
s4
83
s4
94
s4
0/11
0/11
0/11
0/11
0/00
0/00
0/00
0/00
s0
s0
s0
s0
s0
s0
s0
s0
0/00
0/00
0/00
0/00
0/00
0/00
0/00
0
3
16
34
49
80
98
115

12.6 Combining the soft decision outputs yields the following transition probabilities:

	0	1
0	0.909	0.091
1	0.091	0.909

For hard decision decoding, the metric is simply Hamming distance. For the received sequence

$$\mathbf{r} = (11, 10, 00, 01, 10, 01, 00),$$

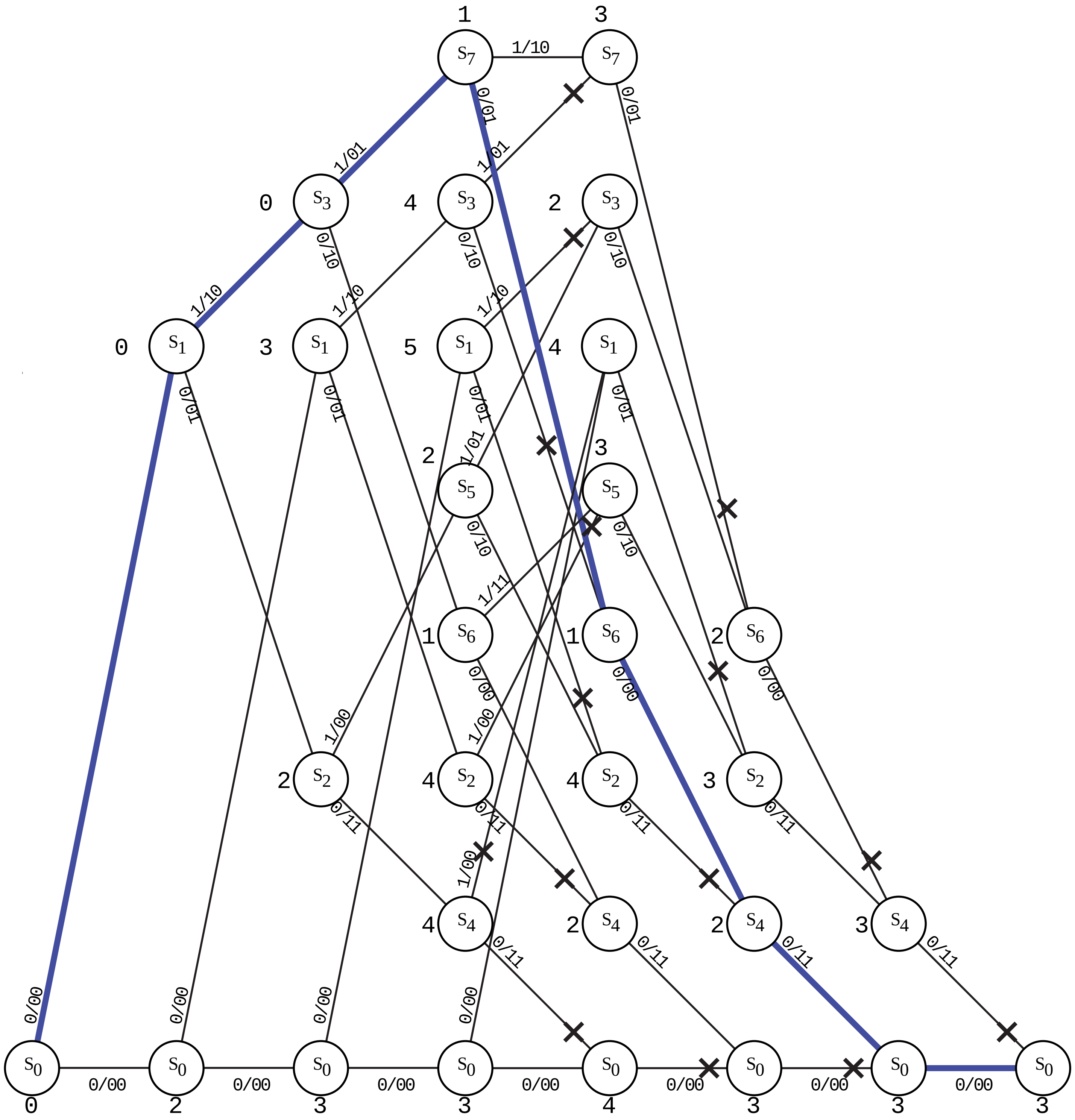
the decoding trellis is as shown in the figure below, and the final survivor is

$$\hat{\mathbf{v}} = (11, 10, 01, 01, 00, 11, 00),$$

which corresponds to the information sequence

$$\hat{\mathbf{u}} = (1110).$$

This result matches the result obtained using soft decisions in Problem 12.5.


1
3
S7
1/10
S7
0/01
0/01
1/01
1/01
0
S3
4
S3
2
S3
0/10
0/10
0/10
1/10
1/10
1/10
0
S1
3
S1
5
S1
4
S1
0/01
0/01
0/01
0/01
2
1/01
3
S5
S5
0/10
0/10
1/11
1
S6
1
S6
2
S6
0/00
0/00
0/00
1/00
1/00
2
S2
4
S2
4
S2
3
S2
0/11
0/11
0/11
0/11
1/00
4
S4
2
S4
2
S4
3
S4
0/11
0/11
0/11
0/11
0/00
0/00
0/00
0/00
S0
S0
S0
S0
S0
S0
S0
S0
0/00
0/00
0/00
0/00
0/00
0/00
0/00
0
2
3
3
4
3
3
3

12.9 **Proof:** For d even,

$$\begin{aligned}
P_d &= \frac{1}{2}\begin{pmatrix} d \\ d/2 \end{pmatrix} p^{d/2}(1-p)^{d/2} + \sum_{e=(d/2)+1}^{d} \begin{pmatrix} d \\ e \end{pmatrix} p^e(1-p)^{d-e} \\
&< \sum_{e=(d/2)}^{d} \begin{pmatrix} d \\ e \end{pmatrix} p^e(1-p)^{d-e} \\
&< \sum_{e=(d/2)}^{d} \begin{pmatrix} d \\ e \end{pmatrix} p^{d/2}(1-p)^{d/2} \\
&= p^{d/2}(1-p)^{d/2} \sum_{e=(d/2)}^{d} \begin{pmatrix} d \\ e \end{pmatrix} \\
&< 2^d p^{d/2}(1-p)^{d/2}
\end{aligned}$$

and thus (12.21) is an upper bound on P_d for d even. Q. E. D.

12.10 The event error probability is bounded by (12.25)

$$P(E) < \sum_{d=d_{free}}^{\infty} A_d P_d < A(X)\big|_{X=2\sqrt{p(1-p)}}.$$

From Example 11.12,

$$A(X) = \frac{X^6 + X^7 - X^8}{1 - 2X - X^3} = X^6 + 3X^7 + 5X^8 + 11X^9 + 25X^{10} + \cdots,$$

which yields

(a) $P(E) < 1.2118 \times 10^{-4}$ for $p = 0.01$,

(b) $P(E) < 7.7391 \times 10^{-8}$ for $p = 0.001$.

The bit error probability is bounded by (12.29)

$$P_b(E) < \sum_{d=d_{free}}^{\infty} B_d P_d < B(X)\big|_{X=2\sqrt{p(1-p)}} = \frac{1}{k}\left.\frac{\partial A(W,X)}{\partial W}\right|_{X=2\sqrt{p(1-p)},W=1}.$$

From Example 11.12,

$$A(W,X) = \frac{WX^7 + W^2(X^6 - X^8)}{1 - W(2X + X^3)} = WX^7 + W^2\left(X^6 + X^8 + X^{10}\right) + W^3\left(2X^7 + 3X^9 + 3X^{11} + X^{13}\right) + \cdots.$$

Hence,

$$\frac{\partial A(W,X)}{\partial W} = \frac{X^7 + 2W(X^6 - 3X^8 - X^{10}) - 3W^2(2X^7 - X^9 - X^{11})}{(1 - 2WX - WX^3)^2} + \cdots$$

and

$$\left.\frac{\partial A(W,X)}{\partial W}\right|_{W=1} = \frac{2X^6 - X^7 - 2X^8 + X^9 + X^{11}}{(1 - 2X - X^3)^2} = 2X^6 + 7X^7 + 18X^8 + \cdots.$$

This yields

(a) $P_b(E) < 3.0435 \times 10^{-4}$ for $p = 0.01$,

(b) $P_b(E) < 1.6139 \times 10^{-7}$ for $p = 0.001$.

12.11 The event error probability is given by (12.26)

$$P(E) \approx A_{d_{free}} \left[2\sqrt{p(1-p)} \right]^{d_{free}} \approx A_{d_{free}} 2^{d_{free}} p^{d_{free}/2}$$

and the bit error probability (12.30) is given by

$$P_b(E) \approx B_{d_{free}} \left[2\sqrt{p(1-p)} \right]^{d_{free}} \approx B_{d_{free}} 2^{d_{free}} p^{d_{free}/2}.$$

From Problem 12.10,

$$d_{free} = 6, \quad A_{d_{free}} = 1, \quad B_{d_{free}} = 2.$$

(a) For $p = 0.01$,

$$P(E) \approx 1 \cdot 2^6 \cdot (0.01)^{6/2} = 6.4 \times 10^{-5}$$

$$P_b(E) \approx 2 \cdot 2^6 \cdot (0.01)^{6/2} = 1.28 \times 10^{-4}.$$

(b) For $p = 0.001$,

$$P(E) \approx 1 \cdot 2^6 \cdot (0.001)^{6/2} = 6.4 \times 10^{-8}$$

$$P_b(E) \approx 2 \cdot 2^6 \cdot (0.001)^{6/2} = 1.28 \times 10^{-7}.$$

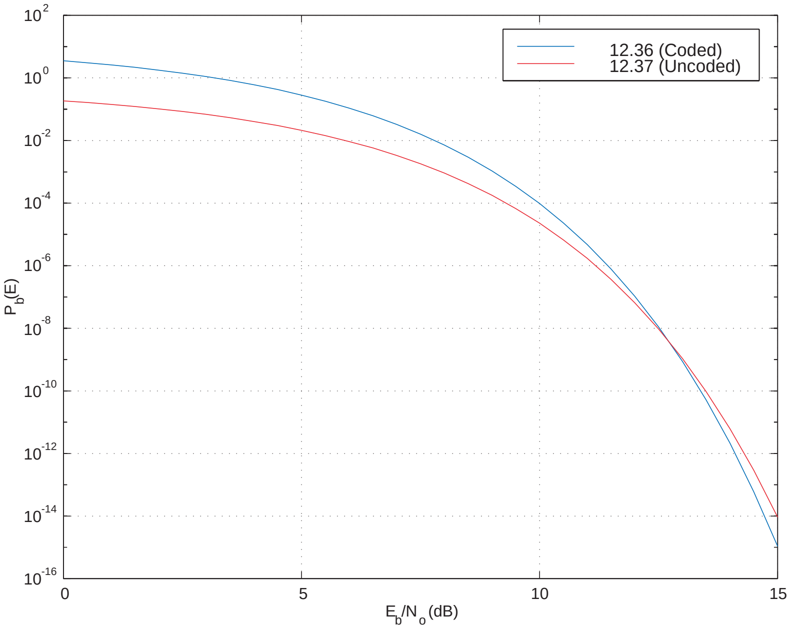
12.12 The $(3,1,2)$ encoder of (12.1) has $d_{free} = 7$ and $B_{d_{free}} = 1$. Thus, expression (12.36) becomes

$$P_b(E) \approx B_{d_{free}} 2^{d_{free}/2} e^{-(R d_{free}/2)\cdot(E_b/N_o)} = 2^{(7/2)} e^{-(7/6)\cdot(E_b/N_o)}$$

and (12.37) remains

$$P_b(E) \approx \frac{1}{2} e^{-E_b/N_o}.$$

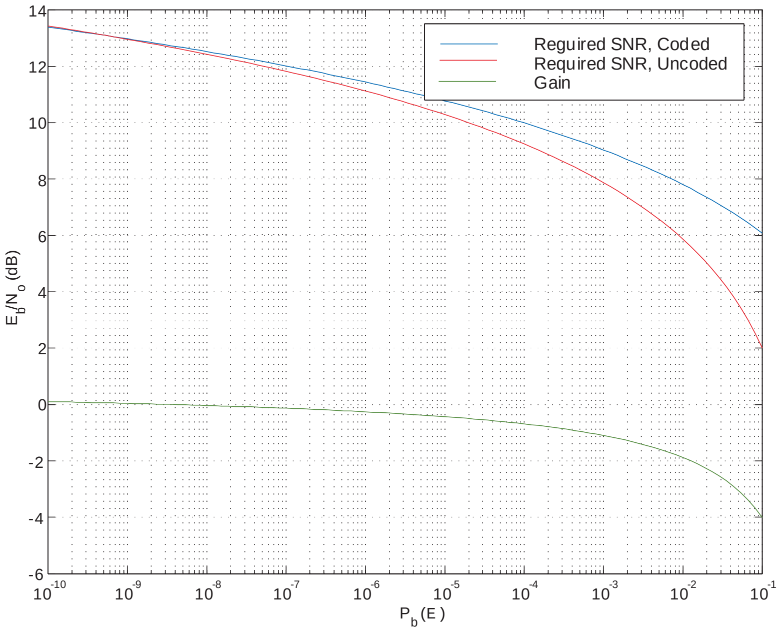
These expressions are plotted versus E_b/N_o in the figure below.


10^2
10^0
10^-2
10^-4
10^-6
10^-8
10^-10
10^-12
10^-14
10^-16
P_b(E)
0
5
10
15
E_b/N_o (dB)
12.36 (Coded)
12.37 (Uncoded)

Equating the above expressions and solving for E_b/N_o yields

$$\begin{aligned}
2^{(7/2)}e^{-(7/6)\cdot(E_b/N_o)} &= \frac{1}{2}e^{-E_b/N_o} \\
1 &= 2^{(9/2)}e^{-(1/6)(E_b/N_o)} \\
e^{(-1/6)(E_b/N_o)} &= 2^{-(9/2)} \\
(-1/6)(E_b/N_o) &= \ln(2^{-(9/2)}) \\
E_b/N_o &= -6\ln(2^{-(9/2)}) = 18.71,
\end{aligned}$$

which is $E_b/N_o = 12.72$dB, the coding threshold. The coding gain as a function of $P_b(E)$ is plotted below.



Note that in this example, a short constraint length code ($\nu = 2$) with hard decision decoding, the approximate expressions for $P_b(E)$ indicate that a positive coding gain is only achieved at very small values of $P_b(E)$, and the asymptatic coding gain is only 0.7dB.

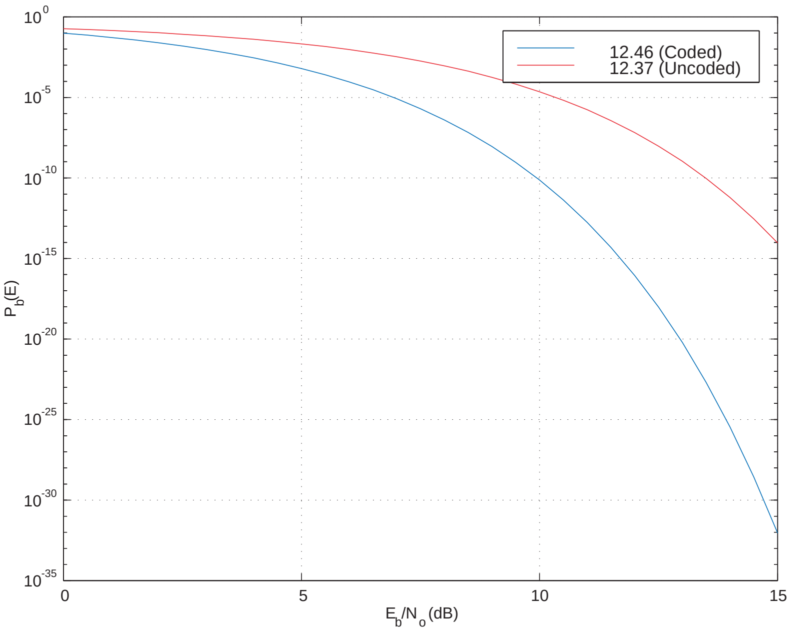
12.13 The $(3,1,2)$ encoder of Problem 12.1 has $d_{free} = 7$ and $B_{d_{free}} = 1$. Thus, expression (12.46) for the unquantized AWGN channel becomes

$$P_b(E) \approx B_{d_{free}}e^{-Rd_{free}E_b/N_o} = e^{-(7/3)\cdot(E_b/N_o)}$$

and (12.37) remains

$$P_b(E) \approx \frac{1}{2}e^{-E_b/N_o}.$$

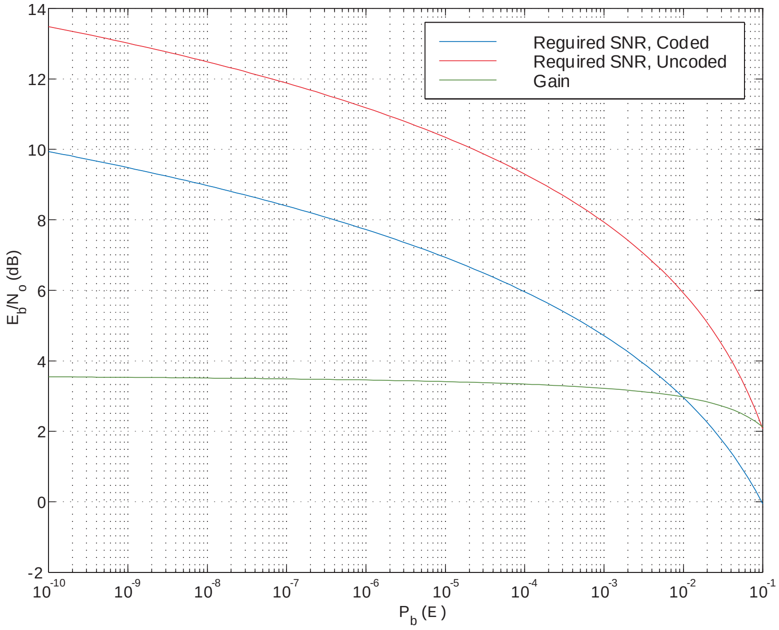
These expressions are plotted versus E_b/N_o in the figure below.



Equating the above expressions and solving for E_b/N_o yields

$$\begin{aligned} e^{-(7/3)\cdot(E_b/N_o)} &= \frac{1}{2}e^{-E_b/N_o} \\ 1 &= \frac{1}{2}e^{(4/3)(E_b/N_o)} \\ e^{(4/3)(E_b/N_o)} &= 2 \\ (4/3)(E_b/N_o) &= \ln(2) \\ E_b/N_o &= (3/4)\ln(2) = 0.5199, \end{aligned}$$

which is $E_b/N_o = -2.84dB$, the coding threshold. (Note: If the slightly tighter bound on $Q(x)$ from (1.5) is used to form the approximate expressin for $P_b(E)$, the coding threshold actually moves to $-\infty\ dB$. But this is just an artifact of the bounds, which are not tight for small values of E_b/N_o.) The coding gain as a function of $P_b(E)$ is plotted below. Note that in this example, a short constraint length code ($\nu = 2$) with soft decision decoding, the approximate expressions for $P_b(E)$ indicate that a coding gain above 3.0 dB is achieved at moderate values of $P_b(E)$, and the asymptotic coding gain is 3.7 dB.


Reguired SNR, Coded
Required SNR, Uncoded
Gain
14
12
10
8
6
4
2
0
-2
E_b/N_o (dB)
10^{-10}
10^{-9}
10^{-8}
10^{-7}
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
P_b (E)

12.14 The IOWEF function of the $(3, 1, 2)$ encoder of (12.1) is

$$A(W, X) = \frac{WX^7}{1 - WX - WX^3}$$

and thus (12.39b) becomes

$$P_b(E) < B(X)|_{X=D_o} = \frac{1}{k} \left. \frac{\partial A(W, X)}{\partial W} \right|_{X=D_0, W=1} = \left. \frac{X^7}{(1 - WX - WX^3)^2} \right|_{X=D_0, W=1}.$$

For the DMC of Problem 12.4, $D_0 = 0.42275$ and the above expression becomes

$$P_b(E) < 9.5874 \times 10^{-3}.$$

If the DMC is converted to a BSC, then the resulting crossover probability is $p = 0.091$. Using (12.29) yields

$$P_b(E) < B(X)|_{X=D_o} = \frac{1}{k} \left. \frac{\partial A(W, X)}{\partial W} \right|_{X=2\sqrt{p(1-p)}, W=1} = \left. \frac{X^7}{(1 - WX - WX^3)^2} \right|_{X=2\sqrt{p(1-p)}, W=1} = 3.7096 \times 10^{-1},$$

about a factor of 40 larger than the soft decision case.

12.16 For the optimum $(2, 1, 7)$ encoder in Table 12.1(c), $d_{free} = 10$, $A_{d_{free}} = 1$, and $B_{d_{free}} = 2$.

(a) From Table 12.1(c)

$$\gamma = 6.99dB.$$

(b) Using (12.26) yields

$$P(E) \approx A_{d_{free}} 2^{d_{free}} p^{d_{free}/2} = 1.02 \times 10^{-7}.$$

(c) Using (12.30) yields

$$P_b(E) \approx B_{d_{free}} 2^{d_{free}} p^{d_{free}/2} = 2.04 \times 10^{-7}.$$

(d) For this encoder

$$\mathbf{G}^{-1} = \begin{bmatrix} D^2 \\ 1 + D^+ D^2 \end{bmatrix}$$

and the amplification factor is $A = 4$.

For the quick-look-in $(2, 1, 7)$ encoder in Table 12.2, $d_{free} = 9$, $A_{d_{free}} = 1$, and $B_{d_{free}} = 1$.

(a) From Table 12.2

$$\gamma = 6.53dB.$$

(b) Using (12.26) yields

$$P(E) \approx A_{d_{free}} 2^{d_{free}} p^{d_{free}/2} = 5.12 \times 10^{-7}.$$

(c) Using (12.30) yields

$$P_b(E) \approx B_{d_{free}} 2^{d_{free}} p^{d_{free}/2} = 5.12 \times 10^{-7}.$$

(d) For this encoder

$$\mathbf{G}^{-1} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

and the amplification factor is $A = 2$.

12.17 The generator matrix of a rate $R = 1/2$ systematic feedforward encoder is of the form

$$\mathbf{G} = \begin{bmatrix} 1 & \mathbf{g}^{(1)}(D) \end{bmatrix}.$$

Letting $\mathbf{g}^{(1)}(D) = 1 + D + D^2 + D^5 + D^7$ achieves $d_{free} = 6$ with $B_{d_{free}} = 1$ and $A_{d_{free}} = 1$.

(a) The soft-decision asymptotic coding gain is

$$\gamma = 4.77dB.$$

(b) Using (12.26) yields

$$P(E) \approx A_{d_{free}} 2^{d_{free}} p^{d_{free}/2} = 6.4 \times 10^{-5}.$$

(c) Using (12.30) yields

$$P_b(E) \approx B_{d_{free}} 2^{d_{free}} p^{d_{free}/2} = 6.4 \times 10^{-5}.$$

(d) For this encoder (and all systematic encoders)

$$\mathbf{G}^{-1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

and the amplification factor is $A = 1$.

12.18 The generator polynomial for the $(15, 7)$ BCH code is

$$\mathbf{g}(X) = 1 + X^4 + X^6 + X^7 + X^8$$

and $d_g = 5$. The generator polynomial of the dual code is

$$\mathbf{h}(X) = \frac{X^{15} + 1}{X^8 + X^7 + X^6 + X^4 + 1} = X^7 + X^6 + X^4 + 1$$

and hence $d_h \geq 4$.

(a) The rate $R = 1/2$ code with composite generator polynomial $\mathbf{g}(D) = 1 + D^4 + D^6 + D^7 + D^8$ has generator matrix

$$\mathbf{G}(D) = \begin{bmatrix} 1 + D^2 + D^3 + D^4 & D^3 \end{bmatrix}$$

and $d_{free} \geq \min(5, 8) = 5$.

(b) The rate $R = 1/4$ code with composite generator polynomial $\mathbf{g}(D) = \mathbf{g}(D^2) + D\mathbf{h}(D^2) = 1 + D + D^8 + D^9 + D^{12} + D^{13} + D^{14} + D^{15} + D^{16}$ has generator matrix

$$\mathbf{G}(D) = \begin{bmatrix} 1 + D^2 + D^3 + D^4 & 1 + D^2 + D^3 & D^3 & D^3 \end{bmatrix}$$

and $d_{free} \geq \min(d_g + d_h, 3d_g, 3d_h) = \min(9, 15, 12) = 9$.

The generator polynomial for the $(31, 16)$ BCH code is

$$\mathbf{g}(X) = 1 + X + X^2 + X^3 + X^5 + X^7 + X^8 + X^9 + X^{10} + X^{11} + X^{15}$$

and $d_g = 7$. The generator polynomial of the dual code is

$$\mathbf{h}(X) = \frac{X^{15}+1}{\mathbf{g}(X)} = X^{16} + X^{12} + X^{11} + X^{10} + X^9 + X^4 + X + 1$$

and hence $d_h \geq 6$.

(a) The rate $R = 1/2$ code with composite generator polynomial $\mathbf{g}(D) = 1 + D + D^2 + D^3 + D^5 + D^7 + D^8 + D^9 + D^{10} + D^{11} + D^{15}$ has generator matrix

$$\mathbf{G}(D) = \begin{bmatrix} 1 + D + D^4 + D^5 & 1 + D + D^2 + D^3 + D^4 + D^5 + D^7 \end{bmatrix}$$

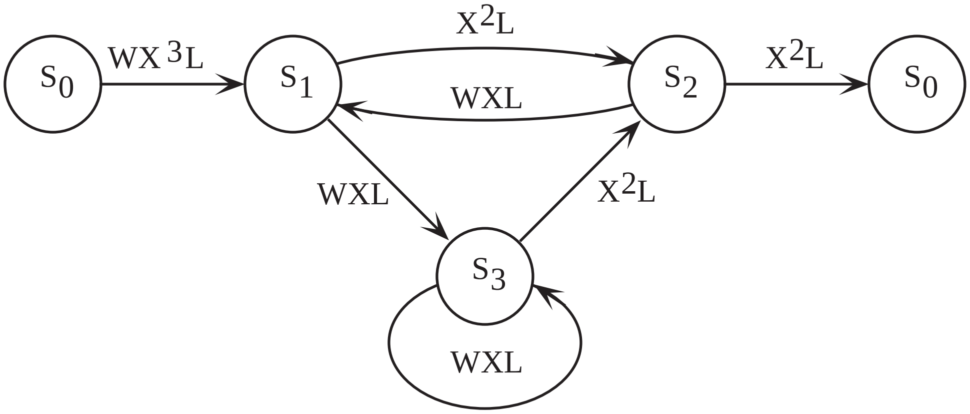
and $d_{free} \geq \min(7, 12) = 7$.

(b) The rate $R = 1/4$ code with composite generator polynomial $\mathbf{g}(D) = \mathbf{g}(D^2) + D\mathbf{h}(D^2) = 1 + D + D^2 + D^3 + D^4 + D^6 + D^9 + D^{10} + D^{14} + D^{16} + D^{18} + D^{19} + D^{20} + D^{21} + D^{22} + D^{23}$ has generator matrix

$$\mathbf{G}(D) = \begin{bmatrix} 1 + D + D^4 + D^5 & 1 + D^2 + D^5 + D^6 + D^8 & 1 + D + D^2 + D^3 + D^4 + D^5 + D^7 & 1 + D^5 \end{bmatrix}$$

and $d_{free} \geq \min(d_g + d_h, 3d_g, 3d_h) = \min(13, 21, 18) = 13$.

12.20 (a) The augmented state diagram is shown below.



The generating function is given by

$$A(W, X, L) = \frac{\sum_i F_i \Delta_i}{\Delta}.$$

There are 3 cycles in the graph:

$$\begin{array}{lll} \text{Cycle 1:} & S_1S_2S_1 & C_1 = WX^3L^2 \\ \text{Cycle 2:} & S_1S_3S_2S_1 & C_2 = W^2X^4L^3 \\ \text{Cycle 3:} & S_3S_3 & C_3 = WXL. \end{array}$$

There is one pair of nontouching cycles:

$$\text{Cycle pair 1:} \quad \text{(loop 1, loop 3)} \quad C_1C_3 = W^2X^4L^3.$$

There are no more sets of nontouching cycles. Therefore,

$$\begin{aligned} \Delta &= 1 - \sum_i C_i + \sum_{i',j'} C_{i'}C_{j'} \\ &= 1 - (WX^3L^2 + W^2X^4L^3 + WXL) + W^2X^4L^3. \end{aligned}$$

There are 2 forward paths:

$$\begin{array}{lll} \text{Forward path 1:} & S_0S_1S_2S_0 & F_1 = WX^7L^3 \\ \text{Forward path 2:} & S_0S_1S_3S_2S_0 & F_2 = W^2X^8L^4. \end{array}$$

Only cycle 3 does not touch forward path 1, and hence

$$\Delta_1 = 1 - WXL.$$

Forward path 2 touches all the cycles, and hence

$$\Delta_2 = 1.$$

Finally, the WEF $A(W, X, L)$ is given by

$$A(W,X,L) = \frac{WX^7L^3(1-WXL) + W^2X^8L^4}{1 - (WX^3L^2 + W^2X^4L^3 + WXL) + W^2X^4L^3} = \frac{WX^7L^3}{1 - WXL - WX^3L^2}$$

and the generating WEF's $A_i(W, X, L)$ are given by:

$$\begin{aligned} A_1(W,X,L) &= \frac{WX^3L(1-WXL)}{\Delta} = \frac{WX^3L(1-WXL)}{1-WXL-WX^3L^2} \\ &= W\,X^3\,L + W^2\,X^6\,L^3 + W^3\,X^7\,L^4 + (W^3X^9\ + W^4X^8\,)\,L^5 + (2\,W^4, X^{10}\ \ + W^5X^9\,)\,L^6 + \cdots \\ A_2(W,X,L) &= \frac{WX^5L^2(1-WXL) + W^2X^6L^3}{\Delta} = \frac{WX^5L^2}{1-WXL-WX^3L^2} \\ &= W\,X^5\,L^2 + W^2\,X^6\,L^3 + (W^2\,X^8 + W^3\,X^7)\,L^4 + (2\,W^3\,X^9 + W^4\,X^8)\,L^5 \\ &\quad +(W^3\,X^{11} + 3\,W^4\,X^{10} + W^5\,X^9)L^6 + \cdots \\ A_3(W,X,L) &= \frac{W^2X^4L^2}{\Delta} = \frac{W^2X^4L^2}{1-WXL-WX^3L^2} \\ &= W^2\,X^4\,L^2 + W^3\,X^5\,L^3 + (W^3\,X^7 + W^4\,X^6)\,L^4 + (2\,W^4\,X^8 + W^5\,X^7)\,L^5 \\ &\quad +(W^4\,X^{10} + 3\,W^5\,X^9 + W^6\,X^8)L^6 \cdots \end{aligned}$$

(b) This code has $d_{free} = 7$, so $\boldsymbol{\tau}_{min}$ is the minimum value of $\boldsymbol{\tau}$ for which $d(\boldsymbol{\tau}) = d_{free} + 1 = 8$. Examining the series expansions of $A_1(W, X, L)$, $A_2(W, X, L)$, and $A_3(W, X, L)$ above yields $\boldsymbol{\tau}_{min} = 5$.

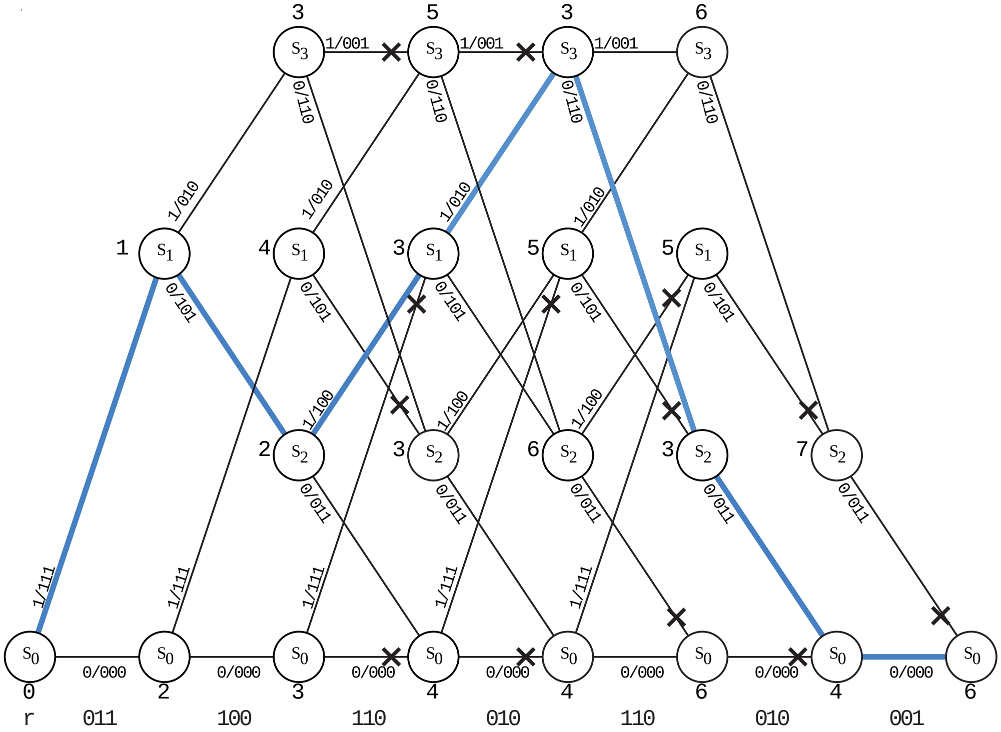
(c) A table of $d(\boldsymbol{\tau})$ and $A_{d(\boldsymbol{\tau})}$ is given below.

$\boldsymbol{\tau}$	$d(\boldsymbol{\tau})$	$A_{d(\boldsymbol{\tau})}$
0	3	1
1	4	1
2	5	1
3	6	1
4	7	1
5	8	1

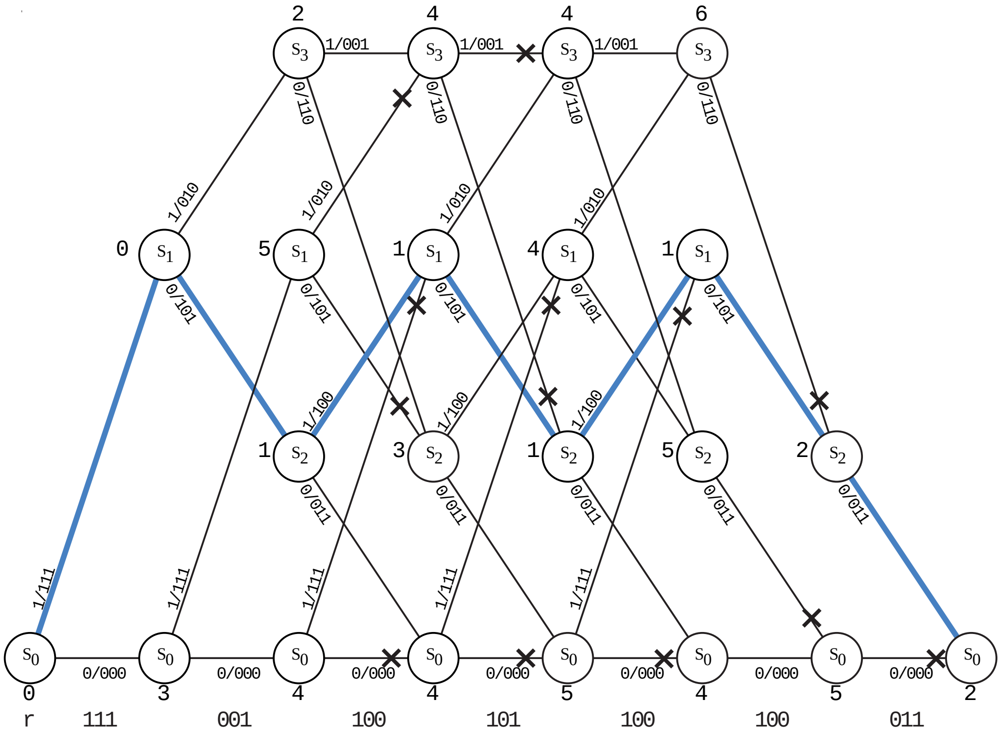
(d) From part (c) and by looking at the series expansion of $A_3(W, X, L)$, it can be seen that

$$\lim_{\boldsymbol{\tau}\to\infty} d(\boldsymbol{\tau}) = \boldsymbol{\tau} + 3.$$

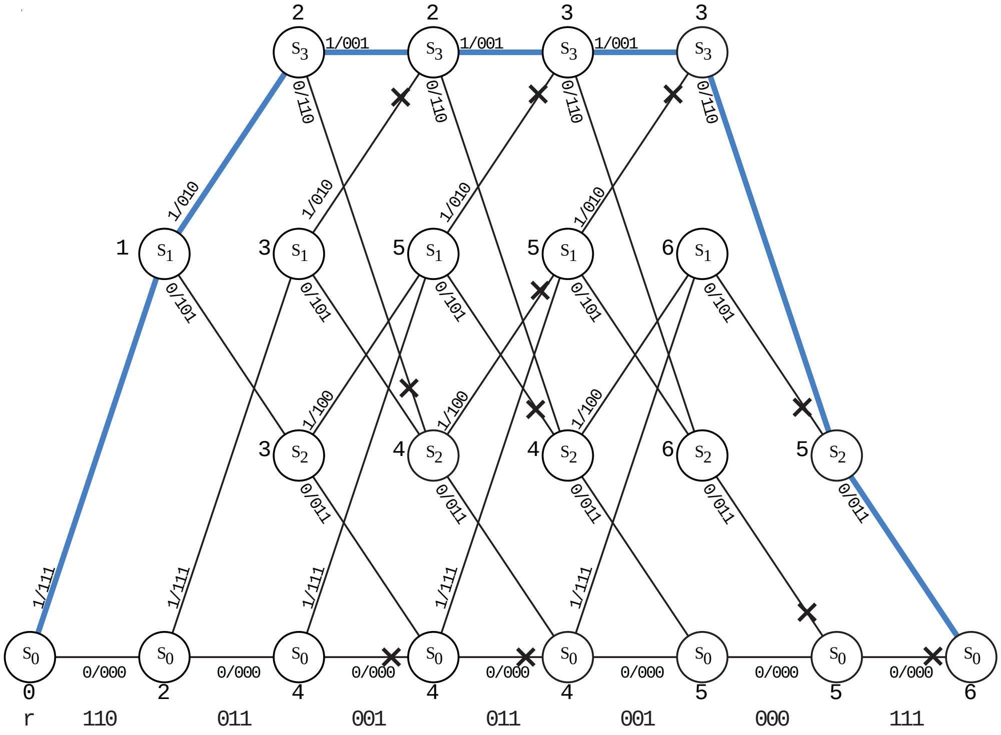
12.21 For a BSC, the trellis diagram of Figure 12.6 in the book may be used to decode the three possible 21-bit subequences using the Hamming metric. The results are shown in the three figures below. Since the **r** used in the middle figure (b) below has the smallest Hamming distance (2) of the three subsequences, it is the most likely to be correctly synchronized.



(a)


2
4
4
6
S3
1/001
0/110
1/010
0
5
1
4
1
S1
0/101
1/100
1
3
1
5
2
S2
0/011
1/111
S0
0/000
0
3
4
4
5
4
5
2
r
111
001
100
101
100
100
011

(b)


2
2
3
3
S3
1/001
S3
1/001
S3
1/001
S3
0/110
0/110
0/110
0/110
1/010
1/010
1/010
1/010
1
3
5
5
6
S1
S1
S1
S1
S1
0/101
0/101
0/101
0/101
0/101
1/100
1/100
1/100
3
4
4
6
5
S2
S2
S2
S2
S2
0/011
0/011
0/011
0/011
0/011
1/111
1/111
1/111
1/111
1/111
S0
0/000
S0
0/000
S0
0/000
S0
0/000
S0
0/000
S0
0/000
S0
0/000
S0
0
2
4
4
4
5
5
6
r
110
011
001
011
001
000
111

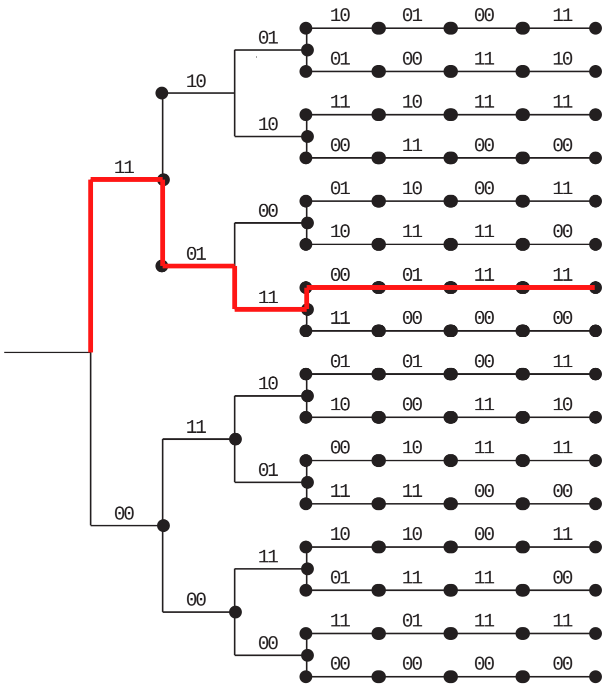
(c)

Chapter 13

Suboptimum Decoding of Convolutional Codes

13.1 (a) Referring to the state diagram of Figure 11.13a, the code tree for an information sequence of length $h = 4$ is shown below.

(b) For $\mathbf{u} = (1001)$, the corresponding codeword is $\mathbf{v} = (11, 01, 11, 00, 01, 11, 11)$, as shown below.



13.2 **Proof:** A binary-input, Q-ary-output DMC is symmetric if

$$P(r_\ell = j|0) = P(r_\ell = Q-1-j|1) \qquad \text{(a-1)}$$

for $j = 0, 1, \ldots, Q-1$. The output probability distribution may be computed as

$$P(r_\ell = j) = \sum_{i=0}^{1} P(r_\ell = j|i)P(i),$$

where i is the binary input to the channel. For equally likely input signals, $P(1) = P(0) = 0.5$ and

$$\begin{aligned} P(r_\ell = j) &= P(r_\ell = j|0)P(0) + P(r_\ell = j|1)P(1) \\ &= 0.5\,[P(r_\ell = j|0) + P(r_\ell = j|1)] \\ &= 0.5\,[P(r_\ell = Q-1-j|0) + P(r_\ell = Q-1-j|1)] \;\; \text{[using (a-1)]} \\ &= P(r_\ell = Q-1-j). \end{aligned}$$

Q. E. D.

13.3 (a) Computing the Fano metric with $p = 0.045$ results in the metric table:

	0	1
0	0.434	-3.974
1	-3.974	0.434

Dividing by 0.434 results in the following integer metric table:

	0	1
0	1	-9
1	-9	1

(b) Decoding $\mathbf{r} = (11, 00, 11, 00, 01, 10, 11)$ using the stack algorithm results in the following eight steps:

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
1(-2)	11(-6)	10(-6)	100(-4)	1001(-2)	10010(0)	100100(-8)	1001000(-6)
0(-18)	10(-6)	111(-14)	111(-14)	111(-14)			
	0(-18)	110(-14)	110(-14)	110(-14)			
		0(-18)	0(-18)	0(-18)			
			101(-24)	1000(-22)			
				101(-24)			

The decoded sequence is $\hat{\mathbf{v}} = (11, 01, 11, 00, 01, 11, 11)$ and $\hat{\mathbf{u}} = [1001]$. The Viterbi algorithm requires fifteen steps to decode the same sequence.

(c) Decoding $\mathbf{r} = (11, 10, 00, 01, 10, 01, 00)$ using the stack algorithm results in the following sixteen steps:

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7	Step 8
1(-2)	11(4)	111(-4)	1110(-2)	110(-4)	11100(-10)	1100(-12)	1101(-12)
0(-18)	10(-16)	110(-4)	110(-4)	11100(-10)	1100(-12)	1101(-12)	10(-16)
	0(-18)	10(-16)	10(-16)	10(-16)	1101(-12)	10(-16)	111000(-18)
		0(-18)	0(-18)	0(-18)	10(-16)	111000(-18)	0(-16)
			1111(-22)	1111(-22)	0(-18)	0(-18)	11000(-20)

Step 9	Step 10	Step 11	Step 12	Step 13	Step 14	Step 15	Step 16
11010(-10)	10(-16)	101(-14)	1011(-12)	10110(-10)	101100(-18)	111000(-18)	1110000(-16)
10(-16)	111000(-18)	111000(-18)	111000(-18)	111000(-18)	111000(-18)	110100(-18)	110100(-18)
111000(-18)	110100(-18)	110100(-18)	110100(-18)	110100(-18)	110100(-18)	0(-18)	0(-18)
0(-18)	0(-18)	0(-18)	0(-18)	0(-18)	0(-18)	11000(-20)	11000(-20)
11000(-20)	11000(-20)	11000(-20)	11000(-20)	11000(-20)	11000(-20)	1010(-32)	1010(-32)
		100(-34)	1010(-32)	1010(-32)	1010(-32)	100(-34)	100(-34)
			100(-34)	100(-34)	100(-34)	1011000(-36)	1011000(-36)

The decoded sequence is $\hat{\mathbf{v}} = (11, 10, 01, 01, 00, 11, 00)$ and $\hat{\mathbf{u}} = (1110)$. This agrees with the result of Problem 12.6.

13.4 (a) Computing the Fano metric using

$$M(r_\ell|v_\ell) = \log_2 \frac{P(r_\ell|v_\ell)}{P(r_\ell)} - R$$

with $R = 1/2$ and

$$\begin{aligned} P(0_1) = \quad & P(1_1) = \quad 0.218 \\ P(0_2) = \quad & P(1_2) = \quad 0.1025 \\ P(0_3) = \quad & P(1_3) = \quad 0.095 \\ P(0_4) = \quad & P(1_4) = \quad 0.0845 \end{aligned}$$

results in

	0_1	0_2	0_3	0_4	1_4	1_3	1_2	1_1
0	0.494	0.443	0.314	-0.106	-1.043	-2.66	-4.07	-7.268
1	-7.268	-4.07	-2.66	-1.043	-0.106	0.314	0.443	0.494

Multiplying by 3/0.106 yields the following integer metric table:

	0_1	0_2	0_3	0_4	1_4	1_3	1_2	1_1
0	14	12	9	-3	-30	-75	-115	-167
1	-167	-115	-75	-30	-3	9	12	14

(b) Decoding $\mathbf{r} = (1_2 1_1, 1_2 0_1, 0_3 0_1, 0_1 1_3, 1_2 0_2, 0_3 1_1, 0_3 0_2)$ using the stack algorithm results in the following thirteen steps:

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6	Step 7
1(26)	11(52)	110(-9)	1100(-70)	111(-106)	1110(-83)	1101(-167)
0(-282)	10(-256)	111(-106)	111(-106)	1101(-167)	11000(-173)	11100(-186)
	0(-282)	10(-256)	1101(-167)	11000(-173)	11000(-173)	11100(-186)
		0(-252)	10(-256)	10(-256)	10(-256)	10(-256)
			0(-282)	0(-282)	0(-282)	0(-282)
					1111(-348)	1111(-348)

Step 8	Step 9	Step 10	Step 11	Step 12	Step 13
11010(-143)	11000(-173)	11100(-186)	110100(-204)	111000(-247)	1110000(-226)
11000(-173)	11100(-186)	110100(-204)	111000(-247)	10(-256)	
11100(-186)	110100(-204)	10(-256)	10(-256)	0(-282)	
10(-256)	10(-256)	0(-282)	0(-282)	110000(-348)	
0(-282)	0(-282)	110000(-331)	110000(-331)	1111(-348)	
1111(-348)	1111(-348)	1111(-348)	1111(-348)	1101000(-394)	

The decoded sequence is $\hat{\mathbf{v}} = (11, 10, 01, 01, 00, 11, 00)$ and $\hat{\mathbf{u}} = (1110)$. This agrees with the result of Problem 12.5(b).

13.6 As can be seen from the solution to Problem 13.3, the final decoded path never falls below the second stack entry (part (b)) or the fourth stack entry (part(c)). Thus, for a stacksize of 10 entries, the final decoded path is not effected in either case.

13.7 From Example 13.5, the integer metric table is

	0	1
0	1	-5
1	-5	1

(a) Decoding the received sequence $\mathbf{r} = (010, 010, 001, 110, 100, 101, 011)$ using the stack bucket algorithm with an interval of 5 results in the following decoding steps:

	Interval 1	Interval 2	Interval 3	Interval 4	Interval 5	Interval 6	Interval 7
	9 to 5	4 to 0	-1 to -5	-6 to -10	-11 to -15	-16 to -20	-21 to -25
Step 1			0(-3)	1(-9)			

Step 2				00(-6)
				1(-9)
					01(-12)		

Step 3				1(-9)	000(-12)
					001(-15)
					01(-12)		

Step 4				11(-6)	000(-12)
					001(-15)
					01(-12)
							10(-24)

Step 5			111(-3)		000(-12)
					001(-15)
					01(-12)
							110(-21)
							10(-24)

Step 6		1110(0)			000(-12)
					001(-15)
					01(-12)
						1111(-18)	110(-21)
							10(-24)

Step 7		11101(3)			11100(-15)
					000(-12)
					001(-15)
					01(-12)
						1111(-18)	110(-21)
							10(-24)

Step 8	111010(6)				11100(-15)
					000(-12)
					001(-15)
					01(-12)
						1111(-18)	110(-21)
							10(-24)

Step 9	1110100(6)				11100(-15)
					000(-12)
					001(-15)
					01(-12)
						1111(-18)	110(-21)
							10(-24)

The decoded sequence is $\hat{\mathbf{v}} = (111, 010, 001, 110, 100, 101, 011)$ and $\hat{\mathbf{u}} = (11101)$, which agrees with the result of Example 13.5.

(b) Decoding the received sequence $\mathbf{r} = (010, 010, 001, 110, 100, 101, 011)$ using the stack bucket algorithm with an interval of 9 results in the following decoding steps.

	Interval 1	Interval 2	Interval 3	Interval 4
	8 to 0	-1 to -9	-10 to -18	-19 to -27
Step 1		0(-3)		
		1(-9)		
Step 2		00(-6)	01(-12)	
		1(-9)		
Step 3		1(-9)	000(-12)	
			001(-15)	
			01(-12)	
Step 4		11(-6)	000(-12)	10(-24)
			001(-15)	
			01(-12)	
Step 5		111(-3)	000(-12)	110(-21)
			001(-15)	10(-24)
			01(-12)	
Step 6	1110(0)		1111(-18)	110(-21)
			000(-12)	10(-24)
			001(-15)	
			01(-12)	
Step 7	11101(3)		11100(-15)	110(-21)
			1111(-18)	10(-24)
			000(-12)	
			001(-15)	
			01(-12)	
Step 8	111010(6)		11100(-15)	110(-21)
			1111(-18)	10(-24)
			000(-12)	
			001(-15)	
			01(-12)	
Step 9	1110100(9)		11100(-15)	110(-21)
			1111(-18)	10(-24)
			000(-12)	
			001(-15)	
			01(-12)	

The decoded sequence is $\hat{\mathbf{v}} = (111, 010, 001, 110, 100, 101, 011)$ and $\hat{\mathbf{u}} = (11101)$, which agrees with the result of Example 13.5 and part (a).

13.8 (i) $\triangle = 5$

Step	Look	M_F	M_B	Node	Metric	T
0	-	-	-	X	0	0
1	LFB	-3	$-\infty$	X	0	-5
2	LFB	-3	-	0	-3	-5
3	LFB	-6	0	X	0	-5
4	LFNB	-9	$-\infty$	X	0	-10
5	LFB	-3	-	0	-3	-10
6	LFB	-6	-	00	-6	-10
7	LFB	-9	-	000	-9	-10
8	LFB	-12	-9	00	-6	-10
9	LFNB	-15	-3	0	-3	-10
10	LFNB	-12	0	X	0	-10
11	LFNB	-9	-	1	-9	-10
12	LFB	-6	-	11	-6	-10
13	LFB	-3	-	111	-3	-5
14	LFB	0	-	1110	0	0
15	LFB	3	-	11101	3	0
16	LFB	6	-	111010	6	5
17	LFB	9	-	1110100	9	Stop

The decoded sequence is $\hat{\mathbf{v}} = (111, 010, 001, 110, 100, 101, 011)$ and $\hat{\mathbf{u}} = [11101]$ which agrees with the result of Example 13.5.

(ii) $\triangle = 10$

Step	Look	M_F	M_B	Node	Metric	T
0	-	-	-	X	0	0
1	LFB	-3	$-\infty$	X	0	-10
2	LFB	-3	-	0	-3	-10
3	LFB	-6	-	00	-6	-10
4	LFB	-9	-	000	-9	-10
5	LFB	-12	-6	00	-6	-10
6	LFNB	-15	-3	0	-3	-10
7	LFNB	-12	0	X	0	-10*
8	LFNB	-9	-	1	-9	-10
9	LFB	-6	-	11	-6	-10
10	LFB	-3	-	111	-3	-10
11	LFB	0	-	1110	0	0
12	LFB	3	-	11101	3	0
13	LFB	6	-	111010	6	0
14	LFB	9	-	1110100	9	Stop

* Not the first visit. Therefore no tightening is done.

Note: The final decoded path agrees with the results of Examples 13.7 and 13.8 and Problem 13.7. The number of computations in both cases is reduced compared to Examples 13.7 and 13.8.

13.20 (a)

$$g^{(1)}(D) = 1 + D + D^3 + D^5 + D^8 + D^9 + D^{10} + D^{11}$$

Therefore:

$$H = \left[\begin{array}{cccccccccccccccccc}
1 & 1 & & & & & & & & & & & & & & & & \\
1 & 0 & 1 & 1 & & & & & & & & & & & & & & \\
0 & 0 & 1 & 0 & 1 & 1 & & & & & & & & & & & & \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & & & & & & & & & & \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \ddots & & & & & & & & & \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & \ddots & & & & & & & & \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & & & \ddots & & & & & & & \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & & & & \ddots & & & & & & \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & & & & & \ddots & & & & & \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & & & & & & \ddots & & & & \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & & & & & & & 1 & 1 & & \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & 0 & 1 & 1
\end{array}\right]$$

(b) Using the parity triangle of the code, we obtain:

$$\begin{array}{lcccccccccccccc}
s_0 = & e_0^{(0)} & & & & & & & & & & & & & +e_0^{(1)} \\
s_1 = & e_0^{(0)} & +e_1^{(0)} & & & & & & & & & & & & +e_1^{(1)} \\
s_2 = & & +e_1^{(0)} & +e_2^{(0)} & & & & & & & & & & & +e_2^{(1)} \\
s_3 = & e_0^{(0)} & & +e_2^{(0)} & +e_3^{(0)} & & & & & & & & & & +e_3^{(1)} \\
s_4 = & & +e_1^{(0)} & & +e_3^{(0)} & +e_4^{(0)} & & & & & & & & & +e_4^{(1)} \\
s_5 = & e_0^{(0)} & & +e_2^{(0)} & & +e_4^{(0)} & +e_5^{(0)} & & & & & & & & +e_5^{(1)} \\
s_6 = & & +e_1^{(0)} & & +e_3^{(0)} & & +e_5^{(0)} & +e_6^{(0)} & & & & & & & +e_6^{(1)} \\
s_7 = & & & +e_2^{(0)} & & +e_4^{(0)} & & +e_6^{(0)} & +e_7^{(0)} & & & & & & +e_7^{(1)} \\
s_8 = & e_0^{(0)} & & & +e_3^{(0)} & & +e_5^{(0)} & & +e_7^{(0)} & +e_8^{(0)} & & & & & +e_8^{(1)} \\
s_9 = & e_0^{(0)} & +e_1^{(0)} & & & +e_4^{(0)} & & +e_6^{(0)} & & +e_8^{(0)} & +e_9^{(0)} & & & & +e_9^{(1)} \\
s_{10} = & e_0^{(0)} & +e_1^{(0)} & +e_2^{(0)} & & & +e_5^{(0)} & & +e_7^{(0)} & & +e_9^{(0)} & +e_{10}^{(0)} & & & +e_{10}^{(1)} \\
s_{11} = & e_0^{(0)} & +e_1^{(0)} & +e_2^{(0)} & +e_3^{(0)} & & & +e_6^{(0)} & & +e_8^{(0)} & & +e_{10}^{(0)} & +e_{11}^{(0)} & & +e_{11}^{(1)}
\end{array}$$

(c) The effect of error bits prior to time unit ℓ are removed. Thus, the modified syndrome bits are given by the following equations:

$$\begin{array}{lllllllllllllll}
s'_{\ell} & = e_{\ell}^{(0)} & & & & & & & & & & & & & \\
s'_{\ell+1} & = e_{\ell}^{(0)} & +e_{\ell+1}^{(0)} & & & & & & & & & & & & +e_{\ell+1}^{(1)} \\
s'_{\ell+2} & = & +e_{\ell+1}^{(0)} & +e_{\ell+2}^{(0)} & & & & & & & & & & & +e_{\ell+2}^{(1)} \\
s'_{\ell+3} & = e_{\ell}^{(0)} & & +e_{\ell+2}^{(0)} & +e_{\ell+3}^{(0)} & & & & & & & & & & +e_{\ell+3}^{(1)} \\
s'_{\ell+4} & = & +e_{\ell+1}^{(0)} & & +e_{\ell+3}^{(0)} & +e_{\ell+4}^{(0)} & & & & & & & & & +e_{\ell+4}^{(1)} \\
s'_{\ell+5} & = e_{\ell}^{(0)} & & +e_{\ell+2}^{(0)} & & +e_{\ell+4}^{(0)} & +e_{\ell+5}^{(0)} & & & & & & & & +e_{\ell+5}^{(1)} \\
s'_{\ell+6} & = & +e_{\ell+1}^{(0)} & & +e_{\ell+3}^{(0)} & & +e_{\ell+5}^{(0)} & +e_{\ell+6}^{(0)} & & & & & & & +e_{\ell+6}^{(1)} \\
s'_{\ell+7} & = & & +e_{\ell+2}^{(0)} & & +e_{\ell+4}^{(0)} & & +e_{\ell+6}^{(0)} & +e_{\ell+7}^{(0)} & & & & & & +e_{\ell+7}^{(1)} \\
s'_{\ell+8} & = e_{\ell}^{(0)} & & & +e_{\ell+3}^{(0)} & & +e_{\ell+5}^{(0)} & & +e_{\ell+7}^{(0)} & +e_{\ell+8}^{(0)} & & & & & +e_{\ell+8}^{(1)} \\
s'_{\ell+9} & = e_{\ell}^{(0)} & +e_{\ell+1}^{(0)} & & & +e_{\ell+4}^{(0)} & & +e_{\ell+6}^{(0)} & & +e_{\ell+8}^{(0)} & +e_{\ell+9}^{(0)} & & & & +e_{\ell+9}^{(1)} \\
s'_{\ell+10} & = e_{\ell}^{(0)} & +e_{\ell+1}^{(0)} & +e_{\ell+2}^{(0)} & & & +e_{\ell+5}^{(0)} & & +e_{\ell+7}^{(0)} & & +e_{\ell+9}^{(0)} & +e_{\ell+10}^{(0)} & & & +e_{\ell+10}^{(1)} \\
s'_{\ell+11} & = e_{\ell}^{(0)} & +e_{\ell+1}^{(0)} & +e_{\ell+2}^{(0)} & +e_{\ell+3}^{(0)} & & & +e_{\ell+6}^{(0)} & & +e_{\ell+8}^{(0)} & & +e_{\ell+10}^{(0)} & +e_{\ell+11}^{(0)} & & +e_{\ell+11}^{(1)}
\end{array}$$

13.28 (a) Using either of the methods described in Examples 13.15 and 13.16, we arrive at the conclusion that $d_{min} = 7$.

(b) From the parity triangle, we can see that this code is not self-orthogonal (for instance, s_3 and s_5 both check information error bit $e_2^{(0)}$).

(c) From the parity triangle shown below, we see that the maximum number of orthogonal parity checks that can be formed on $e_0^{(0)}$ is 4: $\{s_0, s_1, s_2 + s_{11}, s_5\}$.

$$\begin{array}{lcccccccccccc}
\rightarrow & 1 & & & & & & & & & & & \\
\rightarrow & 1 & \boxed{1} & & & & & & & & & & \\
\rightarrow & 0 & 1 & 1 & & & & & & & & & \\
 & 1 & 0 & 1 & 1 & & & & & & & & \\
 & 0 & 1 & 0 & 1 & 1 & & & & & & & \\
\rightarrow & 1 & 0 & \boxed{1} & 0 & \boxed{1} & \boxed{1} & & & & & & \\
 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & & & & & \\
 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & & & & \\
 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & & & \\
 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & & \\
 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & \\
\rightarrow & 1 & 1 & 1 & \boxed{1} & 0 & 0 & \boxed{1} & 0 & \boxed{1} & 0 & \boxed{1} & \boxed{1}
\end{array}$$

(d) So, because of (c), this code is not completely orthogonalizable.

13.32 (a) According to Table 13.2(a), there is only one rate $R = 1/2$ self orthogonal code with $d_{\min} = 9$: the (2,1,35) code with

$$g^{(1)}(D) = 1 + D^7 + D^{10} + D^{16} + D^{18} + D^{30} + D^{31} + D^{35} \text{and } m^{(a)} = 35.$$

(b) According to Table 13.3(a), there is only one rate $R = 1/2$ orthogonalizable code with $d_{\min} = 9$: the (2,1,21) code with

$$g^{(1)}(D) = 1 + D^{11} + D^{13} + D^{16} + D^{17} + D^{19} + D^{20} + D^{21} \text{and } m^{(b)} = 21.$$

(c) The best rate $R = 1/2$ systematic code with $d_{\min} = 9$ is the (2,1,15) code with

$$g^{(1)}(D) = 1 + D + D^3 + D^5 + D^7 + D^8 + D^{11} + D^{13} + D^{14} + D^{15} \text{and } m^{(c)} = 15^*.$$

(d) According to Table 12.1(c), the best rate $R = 1/2$ nonsystematic code with $d_{free} = 9$ (actually, 10 in this case) is the (2,1,6) code with

$$g^{(0)}(D) = 1 + D + D^2 + D^3 + D^6,\ g^{(1)}(D) = 1 + D^2 + D^3 + D^5 + D^6, \text{and } m^{(d)} = 6.$$

Thus $m^{(d)} \quad < \quad m^{(c)} \quad < \quad m^{(b)} \quad < \quad m^{(a)}$.

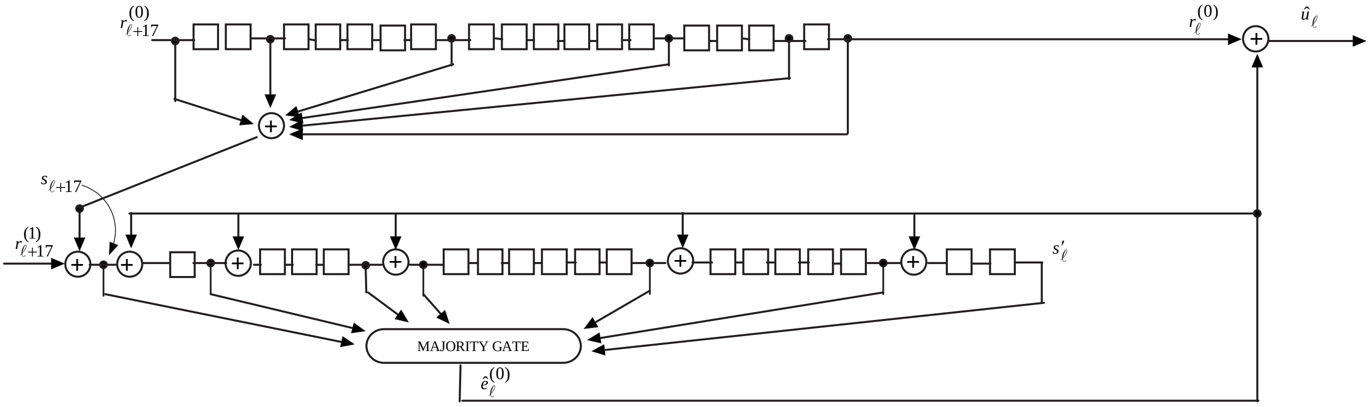
* This generator polynomial can be found in Table 13.1 of the first edition of this text.

13.34 (a) This self orthogonal code with $g^{(1)}(D) = 1+D^2+D^7+D^{13}+D^{16}+D^{17}$ yields the parity triangle:

$$\begin{array}{ccccccccccccccccccc}
\rightarrow & 1 \\
 & 0 & 1 \\
\rightarrow & 1 & 0 & \boxed{1} \\
 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\rightarrow & 1 & 0 & 0 & 0 & 0 & \boxed{1} & 0 & \boxed{1} \\
 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\rightarrow & 1 & 0 & 0 & 0 & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 & \boxed{1} & 0 & \boxed{1} \\
 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
\rightarrow & 1 & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 & \boxed{1} & 0 & \boxed{1} \\
\rightarrow & 1 & \boxed{1} & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \boxed{1} & 0 & 0 & 0 & 0 & \boxed{1} & 0 & \boxed{1}
\end{array}$$

The orthogonal check sums on $e_0^{(0)}$ are $\{s_0, s_2, s_7, s_{13}, s_{16}, s_{17}\}$.

(b) The block diagram of the feedback majority logic decoder for this code is:

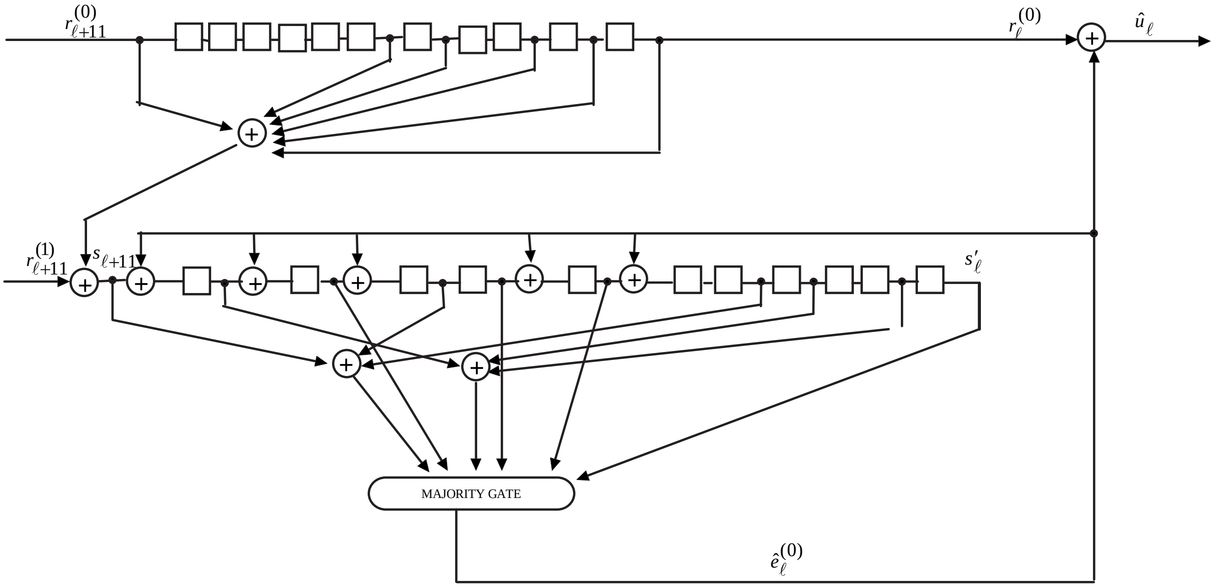


13.37 (a) These orthogonalizable code with $g^{(1)}(D) = 1 + D^6 + D^7 + D^9 + D^{10} + D^{11}$ yields the parity triangle:

$$\begin{array}{cllllllllllll}
\rightarrow & 1 \\
\rightarrow & 0 & 1 \\
 & 0 & 0 & 1 \\
\rightarrow & 0 & 0 & 0 & 1 \\
\rightarrow & 0 & 0 & 0 & 0 & 1 \\
 & 0 & 0 & 0 & 0 & 0 & 1 \\
\rightarrow & 1 & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\
\rightarrow & 1 & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\
 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\
\rightarrow & 1 & 0 & \boxed{1} & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\
\rightarrow & 1 & 1 & 0 & 1 & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \boxed{1} \\
\rightarrow & 1 & 1 & 1 & 0 & 1 & \boxed{1} & 0 & 0 & 0 & 0 & 0 & \boxed{1}
\end{array}$$

The orthogonal check sums on $e_0^{(0)}$ are $\{s_0, s_6, s_7, s_9, s_1 + s_3 + s_{10}, s_4 + s_8 + s_{11}\}$.

(b) The block diagram of the feedback majority logic decoder for this code is:



Chapter 16

Turbo Coding

16.1 Let $\mathbf{u} = [u_0, u_1, \ldots, u_{K-1}]$ be the input to encoder 1. Then

$$\mathbf{v}^{(1)} = [v_0^{(1)}, v_1^{(1)}, \ldots, v_{K-1}^{(1)}] = \mathbf{u}\,\mathbf{G}^{(1)}$$

is the output of encoder 1, where $\mathbf{G}^{(1)}$ is the $K \times K$ parity generator matrix for encoder 1, i.e., $\mathbf{v}^{(1)} = \mathbf{u}\mathbf{G}^{(1)}$ is the parity sequence produced by encoder 1. For example, for the (2,1,2) systematic feedbacK encoder with

$$\mathbf{G}^{(1)}(D) = \begin{bmatrix} 1 & \qquad \dfrac{1+D^2}{1+D+D^2} \end{bmatrix},$$

the parity generator matrix is given by

$$\mathbf{G}^{(1)} = \left[\begin{array}{cccccccccccccc} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \ldots & \ldots & \ldots & \ldots & \ldots \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \ldots & \ldots & \ldots & \ldots \\ & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & \ldots & \ldots & \ldots \\ & & & \ddots & & & & & & & & & & \end{array}\right]. \qquad (K \times K)$$

Now let $\mathbf{u}' = [u_0', u_1', \ldots, u_{K-1}']$ be the (interleaved) input to encoder 2. Then we can write

$$\mathbf{u}' = \mathbf{u}\,\mathbf{T},$$

where $\mathbf{T}$ is a $K \times K$ permutation matrix with a single one in each row and column. (If $\mathbf{T}$ is the identity matrix, then $\mathbf{u}' = \mathbf{u}$.)

The output of encoder 2 is then given by

$$\mathbf{v}^{(2)} = [v_0^{(2)}, v_1^{(2)}, \ldots, v_{K-1}^{(2)}] = \mathbf{u}'\,\mathbf{G}^{(2)} = \mathbf{u}\,\mathbf{T}\,\mathbf{G}^{(2)},$$

where $\mathbf{G}^{(2)}$ is the $K \times K$ parity generator matrix for encoder 2.

Now consider two input sequences $\mathbf{u}_1$ and $\mathbf{u}_2$, both of length K. The corresponding encoder outputs in each case are given by the 3-tuples

$$[\mathbf{u}_1, \mathbf{u}_1\,\mathbf{G}^{(1)}, \mathbf{u}_1'\,\mathbf{G}^{(2)}] = [\mathbf{u}_1,\ \mathbf{u}_1\,\mathbf{G}^{(1)}, \mathbf{u}_1\,\mathbf{T}\,\mathbf{G}^{(2)}] \stackrel{\triangle}{=} \mathbf{y}_1$$

and

$$[\mathbf{u}_2, \mathbf{u}_2\,\mathbf{G}^{(1)}, \mathbf{u}_2'\,\mathbf{G}^{(2)}] = [\mathbf{u}_2,\ \mathbf{u}_2\,\mathbf{G}^{(1)}, \mathbf{u}_2\,\mathbf{T}\,\mathbf{G}^{(2)}] \stackrel{\triangle}{=} \mathbf{y}_2.$$

Now consider the input sequence $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$. The encoder output 3-tuple in this case is given by

$$\begin{aligned}
[\mathbf{u}, \mathbf{u}\,\mathbf{G}^{(1)}, \mathbf{u}'\,\mathbf{G}^{(2)}] &= [\mathbf{u},\ \mathbf{u}\,\mathbf{G}^{(1)}, \mathbf{u}\,\mathbf{T}\,\mathbf{G}^{(2)}] \\
&= [\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_1\,\mathbf{G}^{(1)} + \mathbf{u}_2\,\mathbf{G}^{(2)}, \mathbf{u}_1\mathbf{T}\,\mathbf{G}^{(2)} + \mathbf{u}_2\mathbf{T}\,\mathbf{G}^{(2)}] \\
&= [\mathbf{u}_1, \mathbf{u}_1\,\mathbf{G}^{(1)}, \mathbf{u}_1\mathbf{T}\,\mathbf{G}^{(2)}] + [\mathbf{u}_2, \mathbf{u}_2\,\mathbf{G}^{(2)}, \mathbf{u}_2\mathbf{T}\,\mathbf{G}^{(2)}] \\
&= \mathbf{y}_1 + \mathbf{y}_2.
\end{aligned}$$

Thus superposition holds and the turbo encoder is linear.

16.3 Define C_1 to be the (7,4,3) Hamming code and C_2 to be the (8,4,4) extended Hamming code.

C_1 Codeword list:

0000000
1101000
0111001
1010001
1011010
0110010
1100011
0001011
1110100
0011100
1001101
1000101
0101110
1000110
1000111
1111111

The CWEF for C_1 is given by

$$\begin{aligned}
A_1^{C_1}(Z) &= 3Z^2 + Z^3 \\
A_2^{C_1}(Z) &= 3Z + 3Z^2 \\
A_3^{C_1}(Z) &= 1 + 3Z \\
A_4^{C_1}(Z) &= Z^3
\end{aligned}$$

C_2 Codeword list:

0000 0000
11010001
01110010
10100011
10110100
01100101
11000110
00010111
11101000
00111001
10011010
10001011
01011100
10001101
10001110
11111111

The CWEF for C_2 is given by

$$\begin{aligned}
A_1^{C_2}(Z) &= 4Z^3\\
A_2^{C_2}(Z) &= 6Z^2\\
A_3^{C_2}(Z) &= 4Z\\
A_4^{C_2}(Z) &= Z^4
\end{aligned}$$

The CWEF for the PCBC is given by equation (16.23) as

$$\begin{aligned}
A_w^{PC}(Z) &= A_w^{C_1}(Z) * \ A_w^{C_2}(Z) / \binom{K}{w}\\
A_1^{PC}(Z) &= (3Z^2 + Z^3)(4Z^3)/4 = 3Z^5 + Z^6\\
A_2^{PC}(Z) &= (3Z + 3Z^2)(6Z^2)/6 = 3Z^3 + 3Z^4\\
A_3^{PC}(Z) &= (1 + 3Z)(4Z)/4 = Z + 3Z^2\\
A_4^{PC}(Z) &= (Z^3)(Z^4)/1 = Z^7
\end{aligned}$$

The bit CWEF's are given by

$$\begin{aligned}
B_w^{PC}(Z) &= \left(\frac{w}{K}\right) A_w^{PC}(Z)\\
B_1^{PC}(Z) &= \left(\frac{1}{4}\right)(3Z^5 + Z^6) = .75\ Z^5 + .25\ Z^6\\
B_2^{PC}(Z) &= \left(\frac{2}{4}\right)(3Z^3 + 3Z^4) = 1.5Z^3 + 1.5Z^4\\
B_3^{PC}(Z) &= \left(\frac{3}{4}\right)(Z + 3Z^2) = .75Z^3 + 2.25Z^2
\end{aligned}$$

$$B_4^{PC}(Z) \quad = \quad \binom{4}{4}(Z^7) = Z^7$$

The IRWEF's are given by
$A^{PC}(W,Z) = W(3Z^5 + Z^6) + W^2(3Z^3 + 3Z^4) + W^3(Z + 3Z^2) + W^7Z^7$
$B^{PC}(W,Z) = W(.75Z^5 + .25Z^6) + W^2(1.5Z^3 + 1.5Z^4) + W^3(.75Z + 2.25Z^2) + W^4Z^7$

To find the WEF's, set $W = Z = X$:
$A^{PC}(X) = X^4 + 6X^5 + 6X^6 + X^7 + X^{11}$
$B^{PC}(X) = .75X^4 + 3.75X^5 + 2.25X^6 + .25X^7 + X^{11}$

16.4 The codeword IRWEF can be found from equation (16.34) as follows:

$$\begin{aligned}
A^{PC}(W,Z) \quad = \quad & W(4.5Z^4 + 3Z^5 + 0.5Z^6) + \\
& W^2(1.29Z^2 + 2.57Z^3 + 1.29Z^4 + 3.86Z^5 + 6.43Z^6 + 3Z^7 + \\
& 3.32Z^8 + 3.86Z^9 + 1.93Z^{10} + 0.43Z^{11} + 0.04Z^{12}) + \\
& W^3(0.07 + 0.43Z + 0.64Z^2 + 1.29Z^3 + 5.57Z^4 + 5.57Z^5 + \\
& 7.07Z^6 + 15.43Z^7 + 14.14Z^8 + 5.14Z^9 + 0.64Z^{10}) + \\
& W^4(3.21Z^4 + 17.14Z^5 + 29.29Z^6 + 17.14Z^7 + 3.21Z^8) + \\
& W^5(0.64Z^2 + 5.14Z^3 + 14.14Z^4 + 15.43Z^5 + 7.07Z^6 + 5.57Z^7 + \\
& 5.57Z^8 + 1.29Z^9 + 0.64Z^{10} + 0.43Z^{11} + 0.07Z^{12}) + \\
& W^6(0.04 + 0.43Z + 1.93Z^2 + 3.86Z^3 + 3.32Z^4 + 3Z^5 + \\
& 6.43Z^6 + 3.86Z^7 + 1.29Z^8 + 2.57Z^9 + 1.29Z^{10}) + \\
& W^7(0.05Z^6 + 3Z^7 + 4.5Z^8) + W^8Z^{12}
\end{aligned}$$

To find the bit IRWEF, take each term in the expression for $A^{PC}(W,Z)$ and divide by $w/8$, where w is the exponent of W.

$$\begin{aligned}
B^{PC}(W,Z) \quad = \quad & W(0.56Z^4 + 0.38Z^5 + 0.06Z^6) + \\
& W^2(0.32Z^2 + 0.64Z^3 + 0.32Z^4 + 0.97Z^5 + 1.61Z^6 + .75Z^7 + \\
& 0.83Z^8 + 0.97Z^9 + 0.48Z^{10} + 0.11Z^{11} + 0.01Z^{12}) + \\
& W^3(0.003 + 0.16Z + 0.24Z^2 + 0.48Z^3 + 2.09Z^4 + 2.09Z^5 + \\
& 2.65Z^6 + 5.79Z^7 + 5.30Z^8 + 1.93Z^9 + 0.24Z^{10}) + \\
& W^4(1.61Z^4 + 8.57Z^5 + 14.65Z^6 + 8.57Z^7 + 1.61Z^8) + \\
& W^5(0.40Z^2 + 3.21Z^3 + 8.84Z^4 + 9.64Z^5 + 4.42Z^6 + 3.48Z^7 \\
& 3.48Z^8 + 0.81Z^9 + 0.40Z^{10} + 0.27Z^{11} + 0.04Z^{12}) + \\
& W^6(0.03 + 0.32Z + 1.45Z^2 + 2.90Z^3 + 2.49Z^4 + 2.25Z^5 \\
& 4.82Z^6 + 2.90Z^7 + 0.97Z^8 + 1.93Z^9 + 0.97Z^{10}
\end{aligned}$$

$$W^7(0.04Z^6 + 2.63Z^7 + 3.94Z^8) + W^8Z^{12}$$

To find the WEF's, substitute X=W=Z into the equations for the IRWEF's, as shown below.

$$\begin{aligned} A^{PC}(X) &= 0.07X^3 + 1.71X^4 + 7.71X^5 + 5.61X^6 + 11X^7 + 22.29X^8 + 45.21X^9 + \\ &\quad 66.79X^{10} + 44.79X^{11} + 20.14X^{12} + 9.71X^{13} + 9.46X^{14} + 5.14X^{15} + 3X^{16} + \\ &\quad 0.07X^{17} + 1.29X^{18} + X^{20} \end{aligned}$$

$$\begin{aligned} B^{PC}(X) &= 0.03X^3 + 0.48X^4 + 1.45X^5 + 1.21X^6 + 3.84X^7 + 9.96X^8 + 23.71X^9 + \\ &\quad 33.39X^{10} + 21.19X^{11} + 10.71X^{12} + 5.82X^{13} + 5.04X^{14} + 0.96X^{15} + 2.20X^{16} + \\ &\quad 0.04X^{17} + 0.96X^{18} + X^{20} \end{aligned}$$

16.5 Consider using an h-repeated $(n, k, d_{min}) = (7, 4, 3)$ Hamming code as the constituent code, forming an $(h[2n-k], k) = (10h, 4h)$ PCBC. The output consists of the original input bits $\mathbf{u}$, the parity bits from the non-interleaved encoder $\mathbf{v}^{(1)}$, and the parity bits from the interleaved encoder $\mathbf{v}^{(2)}$. For the $h = 4$-repeated PCBC, the IRWEF of the (28,16) constituent code is

$$\begin{aligned} A(W,Z) &= [1 + W(3Z^2 + Z^3) + W^2(3Z + 3Z^2) + W^3(1 + 3Z) + W^4Z^3]^4 - 1 \\ &= W(12Z^2 + 4Z^3) + \\ &\quad W^2(12Z + 12Z^2 + 54Z^4 + 36Z^5 + 6Z^6) + \\ &\quad W^3(4 + 12Z + 108Z^3 + 144Z^4 + 36Z^5 + 108Z^6 + \\ &\qquad 108Z^7 + 36Z^8 + 4Z^9) + \\ &\quad W^4(90Z^2 + 232Z^3 + 90Z^4 + 324Z^5 + 540Z^6 + \\ &\qquad 252Z^7 + 117Z^8 + 108Z^9 + 54Z^{10} + 12Z^{11} + Z^{12}) + \\ &\quad W^5(36Z + 144Z^2 + 108Z^3 + 432Z^4 + 1188Z^5 + 780Z^6 + \\ &\qquad 468Z^7 + 648Z^8 + 432Z^9 + 120Z^{10} + 12Z^{11}) + \\ &\quad W^6(6 + 36Z + 54Z^2 + 324Z^3 + 1296Z^4 + 1296Z^5 + \\ &\qquad 918Z^6 + 1836Z^7 + 1620Z^8 + 556Z^9 + 66Z^{10}) + \\ &\quad W^7(144Z^2 + 780Z^3 + 1188Z^4 + 1080Z^5 + 2808Z^6 + 3456Z^7 + \\ &\qquad 1512Z^8 + 324Z^9 + 108Z^{10} + 36Z^{11} + 4Z^{12}) + \\ &\quad W^8(36Z + 252Z^2 + 540Z^3 + 783Z^4 + 2592Z^5 + 4464Z^6 + \\ &\qquad 2592Z^7 + 783Z^8 + 540Z^9 + 252Z^{10} + 36Z^{11}) + \end{aligned}$$

$$
\begin{aligned}
& W^{9}(4+36Z+108Z^{2}+324Z^{3}+1512Z^{4}+3456Z^{5}+\\
& \quad 2808Z^{6}+1080Z^{7}+1188Z^{8}+780Z^{9}+144Z^{10})+\\
& W^{10}(66Z^{2}+556Z^{3}+1620Z^{4}+1836Z^{5}+918Z^{6}+1296Z^{7}+\\
& \quad 1296Z^{8}+324Z^{9}+54Z^{10}+36Z^{11}+6Z^{12})+\\
& W^{11}(12Z+120Z^{2}+432Z^{3}+648Z^{4}+468Z^{5}+780Z^{6}+\\
& \quad 1188Z^{7}+432Z^{8}+108Z^{9}+144Z^{10}+36Z^{11})+\\
& W^{12}(1+12Z+54Z^{2}+108Z^{3}+117Z^{4}+252Z^{5}+\\
& \quad 540Z^{6}+324Z^{7}+90Z^{8}+232Z^{9}+90Z^{10})+\\
& W^{13}(4Z^{3}+36Z^{4}+108Z^{5}+108Z^{6}+36Z^{7}+\\
& \quad 144Z^{8}+108Z^{9}+12Z^{11}+4Z^{12})+\\
& W^{14}(6Z^{6}+36Z^{7}+54Z^{8}+12Z^{10}+12Z^{11})+\\
& W^{15}(4Z^{9}+12Z^{10})+\\
& W^{16}Z^{12}.
\end{aligned}
$$

The IRWEF's of the (40,16) PCBC are found, using $A_w^{PC}(Z) = \binom{K}{w}^{-1}[A_w(Z)]^2$, where $K = hk = 16$ is the interleaver (and input) length, to be:

$$
\begin{aligned}
A_1^{PC}(Z) &= 9Z^{4}+6Z^{5}+Z^{6}\\
A_2^{PC}(Z) &= 1.2Z^{2}+2.4Z^{3}+1.2Z^{4}+10.8Z^{5}+18Z^{6}+8.4Z^{7}+25.5Z^{8}+32.4Z^{9}+16.2Z^{10}+\\
&\quad 3.6Z^{11}+0.3Z^{12}\\
A_3^{PC}(Z) &= 0.029+0.171Z+0.257Z^{2}+1.543Z^{3}+6.686Z^{4}+6.686Z^{5}+23.914Z^{6}+61.714Z^{7}+\\
&\quad 56.057Z^{8}+61.771Z^{9}+99.686Z^{10}+83.314Z^{11}+54.771Z^{12}+48.343Z^{13}+\\
&\quad 35.229Z^{14}+15.429Z^{15}+3.857Z^{16}+0.514Z^{17}+0.029Z^{18}\\
A_4^{PC}(Z) &= 4.451Z^{4}+22.945Z^{5}+38.475Z^{6}+54.989Z^{7}+140.459Z^{8}+194.637Z^{9}+186.903Z^{10}+\\
&\quad 257.697Z^{11}+294.389Z^{12}+216.831Z^{13}+151.273Z^{14}+117.156Z^{15}+73.844Z^{16}+\\
&\quad 36.316Z^{17}+17.268Z^{18}+8.229Z^{19}+3.155Z^{20}+0.831Z^{21}+\\
&\quad 0.138Z^{22}+0.013Z^{23}+0.001Z^{24}\\
A_5^{PC}(Z) &= 0.297Z^{2}+2.374Z^{3}+6.527Z^{4}+14.242Z^{5}+50.736Z^{6}+112.549Z^{7}+160.615Z^{8}+\\
&\quad 315.099Z^{9}+550.385Z^{10}+579.363Z^{11}+551.505Z^{12}+611.802Z^{13}+540.89Z^{14}+\\
&\quad 360.791Z^{15}+238.088Z^{16}+158.176Z^{17}+80.901Z^{18}+27.297Z^{19}+\\
&\quad 5.670Z^{20}+0.659Z^{21}+0.033Z^{22}
\end{aligned}
$$

$$\begin{aligned}
A_6^{PC}(Z) &= 0.004 + 0.054Z + 0.243Z^2 + 0.971Z^3 + 5.219Z^4 + 17.964Z^5 + 43.615Z^6 + \\
&\quad 133.355Z^7 + 345.929Z^8 + 533.928Z^9 + 682.391Z^{10} + 1030.59Z^{11} + 1269.74Z^{12} + \\
&\quad 1130.6Z^{13} + 993.686Z^{14} + 891.674Z^{15} + 597.803Z^{16} + 255.219Z^{17} + 65.307Z^{18} + \\
&\quad 9.165Z^{19} + 0.544Z^{20} \\
A_7^{PC}(Z) &= 1.813Z^4 + 19.636Z^5 + 83.089Z^6 + 189.189Z^7 + 341.333Z^8 + 694.221Z^9 + \\
&\quad 1194.5Z^{10} + 1462.3Z^{11} + 1702.7Z^{12} + 2064.99Z^{13} + 1874.92Z^{14} + 1101.01Z^{15} + \\
&\quad 456.243Z^{16} + 169.326Z^{17} + 61.439Z^{18} + 18.05Z^{19} + 4.116Z^{20} + 0.906Z^{21} + \\
&\quad 0.189Z^{22} + 0.025Z^{23} + 0.001Z^{24} \\
A_8^{PC}(Z) &= 0.101Z^2 + 1.41Z^3 + 7.955Z^4 + 25.527Z^5 + 67.821Z^6 + 192.185Z^7 + \\
&\quad 454.462Z^8 + 795.877Z^9 + 1316.39Z^{10} + 2201.74Z^{11} + 2743.06Z^{12} + 2201.74Z^{13} + \\
&\quad 1316.39Z^{14} + 795.877Z^{15} + 454.462Z^{16} + 192.185Z^{17} + 67.821Z^{18} + 25.527Z^{19} + \\
&\quad 7.955Z^{20} + 1.41Z^{21} + 0.101Z^{22} \\
A_9^{PC}(Z) &= 0.001 + 0.025Z + 0.189Z^2 + 0.906Z^3 + 4.116Z^4 + 18.05Z^5 + 61.439Z^6 + \\
&\quad 169.326Z^7 + 456.243Z^8 + 1101.01Z^9 + 1874.92Z^{10} + 2064.99Z^{11} + 1702.7Z^{12} + \\
&\quad 1462.3Z^{13} + 1194.5Z^{14} + 694.221Z^{15} + 341.333Z^{16} + 189.189Z^{17} + \\
&\quad 83.089Z^{18} + 19.636Z^{19} + 1.813Z^{20} \\
A_{10}^{PC}(Z) &= 0.544Z^4 + 9.165Z^5 + 65.307Z^6 + 255.219Z^7 + 597.803Z^8 + 891.674Z^9 + \\
&\quad 993.686Z^{10} + 1130.6Z^{11} + 1269.74Z^{12} + 1030.59Z^{13} + 682.391Z^{14} + 533.928Z^{15} + \\
&\quad 345.929Z^{16} + 133.355Z^{17} + 43.615Z^{18} + 17.964Z^{19} + 5.219Z^{20} + 0.971Z^{21} + \\
&\quad 0.243Z^{22} + 0.054Z^{23} + 0.004Z^{24} \\
A_{11}^{PC}(Z) &= 0.033Z^2 + 0.659Z^3 + 5.67Z^4 + 27.297Z^5 + 80.901Z^6 + 158.176Z^7 + \\
&\quad 238.088Z^8 + 360.791Z^9 + 540.89Z^{10} + 611.802Z^{11} + 551.505Z^{12} + 579.363Z^{13} + \\
&\quad 550.385Z^{14} + 315.099Z^{15} + 160.615Z^{16} + 112.549Z^{17} + 50.736Z^{18} + 14.242Z^{19} + \\
&\quad 6.527Z^{20} + 2.374Z^{21} + 0.297Z^{22} \\
A_{12}^{PC}(Z) &= 0.001 + 0.013Z + 0.138Z^2 + 0.831Z^3 + 3.155Z^4 + 8.229Z^5 + 17.268Z^6 + \\
&\quad 36.316Z^7 + 73.844Z^8 + 117.156Z^9 + 151.273Z^{10} + 216.831Z^{11} + 294.389Z^{12} + \\
&\quad 257.697Z^{13} + 186.903Z^{14} + 194.637Z^{15} + 140.459Z^{16} + 54.989Z^{17} + \\
&\quad 38.475Z^{18} + 22.945Z^{19} + 4.451Z^{20} \\
A_{13}^{PC}(Z) &= 0.029Z^6 + 0.514Z^7 + 3.857Z^8 + 15.429Z^9 + 35.229Z^{10} + 48.343Z^{11} + 54.771Z^{12} + \\
&\quad 83.314Z^{13} + 99.686Z^{14} + 61.771Z^{15} + 56.057Z^{16} + 61.714Z^{17} + 23.914Z^{18} +
\end{aligned}$$

$$\begin{aligned}
& 6.686Z^{19} + 6.686Z^{20} + 1.543Z^{21} + 0.257Z^{22} + 0.171Z^{23} + 0.029Z^{24} \\
A_{14}^{PC}(Z) &= 0.3Z^{12} + 3.6Z^{13} + 16.2Z^{14} + 32.4Z^{15} + 25.5Z^{16} + 8.4Z^{17} + 18Z^{18} + \\
& 10.8Z^{19} + 1.2Z^{20} + 2.4Z^{21} + 1.2Z^{22} \\
A_{15}^{PC}(Z) &= Z^{18} + 6Z^{19} + 9Z^{20} \\
A_{16}^{PC}(Z) &= Z^{24}.
\end{aligned}$$

Using a 4x4 row-column (block) interleaver, the minimum distance of the PCBC is 5. This comes from a weight 1 input, resulting in $w_H(\mathbf{u}) = 1$, $w_H(\mathbf{v}^{(1)}) = 2$, and $w_H(\mathbf{v}^{(2)}) = 2$, where $w_H(\mathbf{x})$ is the Hamming weight of $\mathbf{x}$.

16.7 On page 791 in the text, it is explained that "...any multiple error event in a codeword belonging to a terminated convolutional code can be viewed as a succession of single error events separated by sequences of 0's." Another way to look at it is that for convolutional codewords, we start in the zero state and end in the zero state and any multiple error event can be seen as a series of deviations from the zero state. These deviations from the zero state can be separated by any amount of time spent in the zero state. For example, the codeword could have a deviation starting and another deviation ending at the same zero state, or the codeword could stay in the zero state for several input zeros. Likewise the first input bit could take the codeword out of the zero state or the last input bit could be the one to return the codeword to the zero state.

So, if there are h error events with total length λ in a block codeword length K, then there must be $K - \lambda$ times that state 0 occurs or, as explained in the text, $K - \lambda$ 0's. Now, in the codeword, there are $K - \lambda + h$ places where an error event can start, since the remaining $\lambda - h$ places are then determined by the error events. Since there are h events, the number of ways to choose h elements from $N - \lambda + h$ places gives the multiplicity of block codewords for h-error events.

16.8 The IRWEF and WEF for the PCCC in Example 16.6 is found in the same manner as for a PCBC. The following combines the equations in (16.49) for the CWEF's:

$$\begin{aligned}
A^{PC}(W,Z) &= W^2(4Z^8 + 4Z^{10} + Z^{12}) + W^3(1.81Z^4 + 6.74Z^6 + 9.89Z^8 + 6.74Z^{10} + 1.81Z^{12}) + \\
& W^4(0.93Z^4 + 5.93Z^4 + 10.59Z^8 + 4.67Z^{10} + 3.89Z^{12} + 0.67Z^{14} + 0.33Z^{16}) + \\
& W^5(0.33Z^4 + 2.22Z^6 + 6.37Z^8 + 9.33Z^{10} + 6.81Z^{12} + 1.78Z^{14} + 0.15Z^{16}) + \\
& W^6(0.04Z^4 + 1.04Z^6 + 8.15Z^8 + 12.44Z^{10} + 5.33Z^{12}) + W^7(5.44Z^8 + 3.11Z^{10} + \\
& 0.44Z^{12}) + W^9(Z^{12})
\end{aligned}$$

$$\begin{aligned}
A^{PC}(X) &= 1.81X^7 + 0.93X^8 + 7.07X^9 + 9.97X^{10} + 12.11X^{11} + 15.63X^{12} + 13.11X^{13} + \\
& 13.82X^{14} + 15.95X^{15} + 16.33X^{16} + 9.92X^{17} + 6X^{18} + 2.22X^{19} + 0.33X^{20} + 1.15X^{21}
\end{aligned}$$

16.9 The bit IRWEF is given by:

$$\begin{aligned} B^{PC}(W,Z) &= W^2(0.89Z^8+0.89Z^{10}+0.22Z^{12})+W^3(0.60Z^4+2.25Z^6+3.30Z^8+\\ &\quad 2.25Z^{10}+0.60Z^{12})+W^4(0.41Z^4+2.63Z^6+4.71Z^8+2.07Z^{10}+1.73Z^{12}+\\ &\quad 0.30Z^{14}+0.15Z^{16})+W^5(0.19Z^4+1.23Z^6+3.54Z^8+5.18Z^{10}+3.79Z^{12}+\\ &\quad 0.99Z^{14}+0.08Z^{16})+W^6(0.02Z^4+0.69Z^6+5.43Z^8+8.30Z^{10}+3.55Z^{12})+\\ &\quad W^7(4.23Z^8+2.42Z^{10}+0.35Z^{12})+W^9Z^{12} \end{aligned}$$

The bit WEF is given by:

$$\begin{aligned} B^{PC}(X) &= 0.60X^7+0.41X^8+2.43X^9+3.55X^{10}+4.53X^{11}+6.29X^{12}+5.79X^{13}+7.73X^{14}\\ &\quad 10.02X^{15}+10.02X^{16}+6.20X^{17}+3.85X^{18}+1.33X^{19}+0.15X^{20}+1.08X^{21} \end{aligned}$$

16.10 Redrawing the encoder block diagram and the IRWEF state diagram for the reversed generators, we see that the state diagram is essentially the same except that W and Z are switched. Thus, we can use equation (16.41) for the new IRWEF with W and Z reversed.

$$\begin{aligned} A(W,Z,L) &= L^3W^2Z^3+L^4W^4Z^2+L^5(W^4Z^3+W^2Z^4)+L^6(2W^4Z^3+W^4Z^4)+L^7(W^2Z^5+\\ &\quad 2W^4Z^4+W^4Z^5+W^6Z^2)+L^8(W^4Z^5+3W^4Z^4+2W^4Z^5+2W^6Z^3)+L^9(W^2Z^6+\\ &\quad 3W^4Z^5+2W^4Z^6+W^4Z^7+3W^6Z^3+3W^6Z^4). \end{aligned}$$

After dropping all terms of order larger than L^9, the single-error event enumerators are obtained as follows:

$$\begin{array}{llll} A^{(1)}_{2,3}=Z^3 & A^{(1)}_{2,5}=Z^4 & A^{(1)}_{2,7}=Z^5 & A^{(1)}_{2,9}=Z^6 \\ A^{(1)}_{4,4}=Z^2 & A^{(1)}_{4,5}=Z^3 & A^{(1)}_{4,6}=2Z^3+Z^4 & \\ A^{(1)}_{4,7}=2Z^4+Z^5 & A^{(1)}_{4,8}=3Z^4+2Z^5+Z^6 & A^{(1)}_{4,9}=3Z^5+2Z^6+Z^7 & \\ A^{(1)}_{6,7}=Z^2 & A^{(1)}_{6,8}=2Z^3 & A^{(1)}_{6,9}=3Z^3+2Z^4 & \end{array}$$

The double-error event IRWEF is

$$\begin{aligned} A^2(W,Z,L) &= [A(W,Z,L)]^2\\ &= L^6W^4Z^6+2L^7W^6Z^5+L^8(2W^4Z^7+2W^6Z^6+W^8Z^4)+L^9(6W^6Z^6+2W^6Z^7+\\ &\quad 2W^8Z^5)+\ldots \end{aligned}$$

Dropping all terms of order greater than L^9 gives the double-error event enumerators $A^{(2)}_{2,\ell}(Z)$:

$$\begin{array}{lll} A^{(2)}_{4,6}=Z^6 & A^{(2)}_{4,8}=2Z^7 & \\ A^{(2)}_{6,7}=2Z^5 & A^{(2)}_{6,8}=2Z^6 & A^{(2)}_{6,9}=6Z^6+2Z^7 \\ A^{(2)}_{8,8}=Z^4 & A^{(2)}_{8,9}=2Z^5 & \end{array}$$

Following the same procedure, the triple-error event IRWEF is given by $A^{(3)}(W, Z, L) = [A(W, Z, L)]^3 = L^9W^6Z^9 + \ldots$, and the triple-error event enumerator is given by $A^{(3)}_{6,9}(Z) = Z^9$.

Before finding the CWEF's we need to calculate h_{max}. Notice that there are no double-error events of weight less than 4 and that the only triple-error event has weight 6. Also notice that, for the terminated encoder, odd input weights don't appear. So for weight $2, h_{max} = 1$. For weight 4 and $8, h_{max} = 2$. For weight $6, h_{max} = 3$. Now we can use equations (16.37) and (16.39) to find the CWEF's as follows:

$$\begin{aligned}
A_2(Z) &= c[3,1]A^{(1)}_{2,3}(Z) + c[5,1]A^{(1)}_{2,5}(Z) + c[7,1]A^{(1)}_{2,7}(Z) + c[9,1]A^{(1)}_{2,9}(Z) \\
&= 3Z^2 + 7Z^3 + 5Z^4 + Z^6 \\
A_4(Z) &= c[4,1]A^{(1)}_{4,4}(Z) + c[5,1]A^{(1)}_{4,5}(Z) + c[6,1]A^{(1)}_{4,6}(Z) + c[7,1]A^{(1)}_{4,7}(Z) + c[8,1]A^{(1)}_{4,8}(Z) + \\
&\quad c[9,1]A^{(1)}_{4,9}(Z) + c[6,2]A^{(2)}_{4,6}(Z) + c[8,2]A^{(2)}_{4.8}(Z) \\
&= 6Z^2 + 13Z^3 + 16Z^4 + 10Z^5 + 14Z^6 + 7Z^7 \\
A_6(Z) &= c[7,1]A^{(1)}_{6,7}(Z) + c[8,1]A^{(1)}_{6,8}(Z) + c[9,1]A^{(1)}_{6,9}(Z) + C[6,2]A^{(2)}_{6,7}(Z) + c[8,2]A^{(2)}_{6,8}(Z) + \\
&\quad c[9,2]A^{(2)}_{6,9}(Z) + c[9,3]A^{(3)}_{6,9}(Z) \\
&= 3Z^2 + 7Z^3 + 3Z^4 + 12Z^5 + 12Z^6 + 2Z^7 + Z^9 \\
A_8(Z) &= c[8,2]A^{(2)}_{8,8}(Z) + c[9,2]A^{(2)}_{8,9}(Z) \\
&= 3Z^4 + 2Z^5
\end{aligned}$$

A quick calculation shows that the CWEF's include a total of 127 nonzero codewords, the correct number for an (18,7) code.

The IRWEF and WEF are given by:

$$\begin{aligned}
A(W,Z) &= W^2(3Z^2 + 7Z^3 + 5Z^4 + Z^6) + W^4(6Z^2 + 13Z^3 + 16Z^4 + 10Z^5 + 14Z^6 + 7Z^7) + \\
&\quad W^6(3Z^2 + 7Z^3 + 3Z^4 + 12Z^5 + 12Z^6 + 2Z^7 + Z^9) + W^8(3Z^4 + 2Z^5) \\
A(X) &= 3X^4 + 7X^5 + 11X^6 + 13X^7 + 20X^8 + 17X^9 + 17X^{10} + 20X^{11} + 15Z^{12} + 4X^{13} + X^{15}
\end{aligned}$$

This convolutional code has minimum distance 4, one less than for the code of Example 6.6. As in the example, we must modify the concept of the uniform interleaver because we are using convolutional constituent codes. Therefore, note that for weight 2, there are 16 valid input sequences. For weight 4, there are 66. For weight 6, there are 40, and for weight 8, there are 5. For all other weights, there are no valid input sequences.

The CWEF's of the (27,7) PCCC can be found as follows:

$$\begin{aligned}
A_2^{PC}(Z) &= (3Z^2+7Z^3+5Z^4+Z^6)^2/16 \\
&= 0.56Z^4+2.62Z^5+4.94Z^6+4.37Z^7+1.94Z^8+0.87Z^9+0.62Z^{10}+0.06Z^{12} \\
A_4^{PC}(Z) &= (6Z^2+13Z^3+16Z^4+10Z^5+14Z^6+7Z^7)^2/66 \\
&= 0.55Z^4+2.36Z^5+5.47Z^6+8.12Z^7+10.36Z^8+11.63Z^9+11.06Z^{10}+7.65Z^{11} \\
&\quad 5.09Z^{12}+2.97Z^{13}+0.74Z^{14} \\
A_6^{PC}(Z) &= (3Z^2+7Z^3+3Z^4+12Z^5+12Z^6+2Z^7+Z^9)^2/40 \\
&= 0.22Z^4+1.05Z^5+1.67Z^6+2.85Z^7+6.22Z^8+6.3Z^9+6.1Z^{10}+7.65Z^{11}+ \\
&\quad 5.15Z^{12}+1.35Z^{13}+0.7Z^{14}+0.6Z^{15}+0.1Z^{16}+0.02Z^{18} \\
A_8^{PC}(Z) &= (3Z^4+2Z^5)^2/5 \\
&= 1.8Z^8+2.4Z^9+0.8Z^{10}
\end{aligned}$$

16.11 As noted in Problem 16.10, odd input weights do not appear. For weight 2, $h_{max}=1$ and equation (16.55) simplifies to

$$A_2^{PC}(Z)=2[A_2^{(1)}(Z)]^2 \text{ and } B_2^{PC}(Z)=\frac{4}{K}[A_2^{(1)}(Z)]^2.$$

For weight 4 and 8, $h_{max}=2$, so we have

$$\begin{aligned}
A_4^{PC}(Z) &= 6[A_4^{(2)}(Z)]^2 \text{ and } B_4^{PC}(Z)=\frac{24}{K}[A_4^{(2)}(Z)]^2. \\
A_8^{PC}(Z) &= \frac{10080}{K^4}[A_8^{(2)}(Z)]^2 \text{ and } B_4^{PC}(Z)=\frac{80640}{K^5}[A_8^{(2)}(Z)]^2.
\end{aligned}$$

For weight 6, $h_{max}=3$, so

$$A_6^{PC}(Z) = 20[A_6^{(3)}(Z)]^2 \text{ and } B_6^{PC}(Z)=\frac{120}{K}[A_6^{(3)}(Z)]^2.$$

Including only these terms in the approximate IRWEF's for the PCCC gives

$$\begin{aligned}
A(W,Z) &= 2W^2[A_2(Z)]^2+6W^4[A_4(Z)]^2+20W^6[A_6(Z)]^2+\frac{10080W^8}{K^4}[A_8(Z)]^2 \\
&\approx 2W^2[A_2(Z)]^2+6W^4[A_4(Z)]^2+20W^6[A_6(Z)]^2 \\
B(W,Z) &= \frac{4W^2}{K}[A_2(Z)]^2+\frac{24W^4}{K}[A_4(Z)]^2+\frac{120W^6}{K}[A_6(Z)]^2+\frac{80640W^8}{K^5}[A_8(Z)]^2 \\
&\approx \frac{4W^2}{K}[A_2(Z)]^2+\frac{24W^4}{K}[A_4(Z)]^2+\frac{120W^6}{K}[A_6(Z)]^2.
\end{aligned}$$

The approximate CWEF's from the previous problem are:

$$\begin{aligned} A_2(Z) &\approx 3Z^2+7Z^3+5Z^4+Z^6 \\ A_4(Z) &\approx 6Z^2+13Z^3+16Z^4+10Z^5+14Z^6+7Z^7 \\ A_6(Z) &\approx 3Z^2+7Z^3+3Z^4+12Z^5+12Z^6+2Z^7+Z^9 \\ A_8(Z) &\approx 3Z^4+2Z^5. \end{aligned}$$

Now we obtain the approximate IRWEF's as:

$$\begin{aligned} A(W,Z) &\approx 2W^2Z^4(3+7Z+5Z^2+Z^4)^2++6W^4Z^4(6+13Z+16Z^2+10Z^3+14Z^4+7Z^5)^2+ \\ &\quad 20W^6Z^4(3+7Z+3Z^2+12Z^3+12Z^4+2Z^5+Z^7)^2 \\ B(W,Z) &\approx (4W^2Z^4(3+7Z+5Z^2+Z^4)^2+24W^4Z^4(6+13Z+16Z^2+10Z^3+14Z^4+7Z^5)^2+ \\ &\quad 120W^6Z^4(3+7Z+3Z^2+12Z^3+12Z^4+2Z^5+Z^7)^2)/K \end{aligned}$$

and the approximate WEF's are given by:

$$\begin{aligned} A^{PC}(X) &\approx 18X^6+84X^7+374X^8+1076X^9+2408X^{10}+4084X^{11}+5464X^{12}+6888X^{13}+ \\ &\quad 9362X^{14}+8064X^{15}+6896X^{16}+7296X^{17}+4414X^{18}+1080X^{19}+560X^{20}+ \\ &\quad 480X^{21}+80X^{22}+20X^{24} \\ B^{PC}(X) &\approx 36X^6/K+168X^7/K+1180X^8/K+4024X^9/K+9868X^{10}/K+17960X^{11}/K+ \\ &\quad 24496X^{12}/K+32112X^{13}/K+47404X^{14}/K+42336X^{15}/K+37344X^{16}/K+ \\ &\quad 41424X^{17}/K+25896X^{18}/K+6480X^{19}/K+3360X^{20}/K+2880X^{21}/K+ \\ &\quad 480X^{22}/K+120X^{24}/K \end{aligned}$$

16.13 First constituent encoder: $G_{ff}^{(1)}(D) = [1+D+D^2 \qquad 1+D^2]$

Second constituent encoder: $G_{ff}^{(2)}(D) = [1 \qquad 1+D+D^2]$

For the first constituent encoder, the IOWEF is given by

$$A^{C_1}(W,X,L) = WX^5L^3 + W^2L^4(1+L)X^6 + W^3L^5(1+L)^2X^7 + \dots,$$

and for the second one the IRWEF can be computed as

$$A^{C_2}(W,Z,L) = WZ^3L^3 + W^2Z^2L^4 + W^2Z^4L^5 + \dots,$$

The effect of uniform interleaving is represented by

$$A_w^{PC}(X,Z) = \frac{A_w^{C_1}(X) * A_w^{C_2}(Z)}{\binom{K}{w}}$$

and for large K, this can be approximated as

$$A_w^{PC}(X,Z) \approx \sum_{1\leq\ h_1 \leq\ h_{max}} \ \sum_{1\leq\ h_2 \leq\ h_{max}} \frac{c[h_1]c[h_2]}{\binom{K}{w}}\ A_w^{(h_1)}(X)A_w^{(h_2)}(Z),$$

where $A_w^{(h_1)}(X)$ and $A_w^{(h_2)}(Z)$ are the conditional IO and IR h-error event WEF's of the nonsystematic and systematic constituent encoders, C_1 and C_2, respectively. With further approximations, we obtain

$$A_w^{PC}(X,Z) \approx \frac{w!}{h_{1max}!h_{2max}!} K^{(h_{1max}+h_{2max}-w)} A_w^{(h_{1max})}(X) A_w^{(h_{2max})}(Z)$$

and

$$B_w^{PC}(X,Z) \approx \frac{w}{K}\ A_w^{PC}(X,Z).$$

Going directly to the large K case, for any input weight $w, w \geq 1,\ h_{max} = w$, since the weight 1 single error event can be repeated w times. It follows that

$$A_w^{(w)}(X) = X^{5w}, \quad w \geq 1$$

and

$$A_w^{(w)}(Z) = Z^{3w}, \quad w \geq 1.$$

Hence

$$A_w^{PC}(X,Z) \approx \frac{w!}{w!w!} K^{(w+w-w)} X^{5w} Z^{3w} = \frac{K^w}{w!} X^{5w} Z^{3w}$$

and

$$B_w^{PC}(X,Z) \approx \frac{K^{(w-1)}}{(w-1)!} X^{5w} Z^{3w}.$$

Therefore

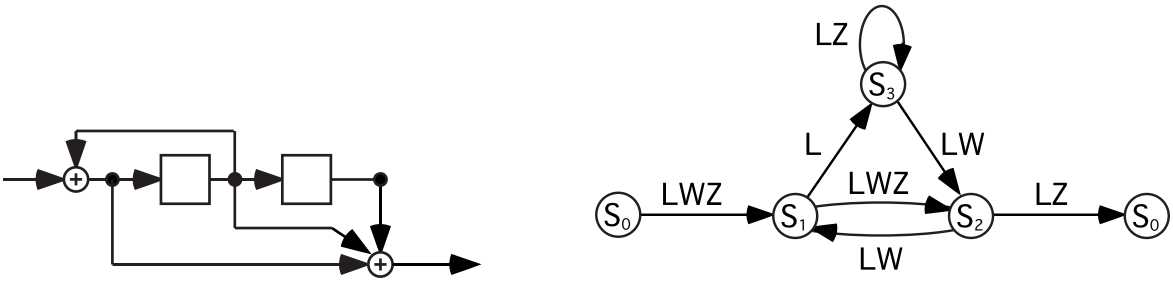
$$\begin{aligned} A^{PC}(W,X) &\approx \textstyle\sum_{1\leq w\leq K} W^w \frac{K^w}{w!} X^{8w} = KWX^8 + \frac{K}{2}^2 W^2 X^{16} + \frac{K}{6}^3 W^3 X^{24} - \ldots, \\ B^{PC}(W,X) &\approx WX^8 + KW^2X^{16} + \frac{K^2}{2} W^3 X^{24} + \ldots, \end{aligned}$$

the average WEF's are

$$\begin{aligned}A^{PC}(X) &= KX^8 + \frac{K^2}{2}X^{16} + \frac{K^3}{6}X^{24} + \dots,\\ B^{PC}(X) &= X^8 + KX^{16} + \frac{K^2}{2}X^{24} + \dots,\end{aligned}$$

and the free distance of the code is 8.

16.14 The encoder and augmented modified state diagram for this problem are shown below:



(a)

(b)

(a) Encoder and (b) Augmented Modified State Diagram for $G(D) = \frac{1+D+D^2}{1+D}$

Note that in order to leave from and return to state S_0 (i.e., terminating a $K-2$ bit input sequence), an even overall-input (including termination bits) weight is required. Examination of the state diagram reveals 6 paths that contain overall-input weight $W < 6$ ("$\cdots$" means an indefinite loop around S_3):

Path	Function
$\{S_0, S_1, S_2, S_0\}$	$L^3W^2Z^3$
$\{S_0, S_1, S_2, S_1, S_2, S_0\}$	$L^5W^4Z^4$
$\{S_0, S_1, S_3, \cdots, S_3, S_2, S_0\}$	$\frac{L^4W^2Z^2}{1-ZL}$
$\{S_0, S_1, S_2, S_1, S_3, \cdots, S_3, S_2, S_0\}$	$\frac{L^6W^4Z^3}{1-ZL}$
$\{S_0, S_1, S_3, \cdots, S_3, S_2, S_1, S_2, S_0\}$	$\frac{L^6W^4Z^3}{1-ZL}$
$\{S_0, S_1, S_3, \cdots, S_3, S_2, S_1, S_3, \cdots, S_3, S_2, S_0\}$	$\frac{L^7W^4Z^2}{(1-ZL)^2}$

resulting in the single error event IRWEF for $W < 6$ of

$$A^{(1)}(W, Z, L) = L^3W^2Z^3 + L^5W^4Z^4 + \frac{L^4W^2Z^2 + 2L^6W^4Z^3}{1-ZL} + \frac{L^7W^4Z^2}{(1-ZL)^2},$$

and for both $W < 6$ and $L < 10$,

$$\begin{aligned} A^{(1)}(W,Z,L) &= L^3W^2Z^3 + L^5W^4Z^4 + \left[\sum_{n=0}^{5} L^{4+n}W^2Z^{2+n}\right] + \\ & \left[2\sum_{n=0}^{3} L^{6+n}W^4Z^{3+n}\right] + \left[\sum_{n=0}^{2}(n+1)L^{7+n}W^4Z^{2+n}\right] \quad . \end{aligned}$$

The IRWEF for double error events for $W < 6$ is then

$$A^{(2)}(W,Z,L) = [A^{(1)}(W,Z,L)]^2 = L^6W^4Z^6 + \frac{2L^7W^4Z^5}{1-ZL} + \frac{L^8W^4Z^4}{(1-ZL)^2},$$

and for both $W < 6$ and $L < 10$,

$$A^{(2)}(W,Z,L) = L^6W^4Z^6 + \left[2\sum_{n=0}^{2} L^{7+n}W^4Z^{5+n}\right] + \left[\sum_{n=0}^{1}(n+1)L^{8+n}W^4Z^{4+n}\right] \quad .$$

Thus the single- and double-error event enumerators for $W < 6$ and $L < 10$ are

$$\begin{array}{lllll} A^{(1)}_{2,3}(Z) = Z^3 & A^{(1)}_{2,4+n}(Z) = Z^{2+n} & & & \\ A^{(1)}_{4,5}(Z) = Z^4 & A^{(1)}_{4,6+n}(Z) = 2Z^{3+n} & A^{(1)}_{4,7}(Z) = Z^2 & A^{(1)}_{4,8}(Z) = 2Z^3 & A^{(1)}_{4,9}(Z) = 3Z^4 \\ A^{(2)}_{4,6}(Z) = Z^6 & A^{(2)}_{4,7+n}(Z) = 2Z^{5+n} & A^{(2)}_{4,8}(Z) = Z^4 & A^{(2)}_{4,9}(Z) = 2Z^5, & \end{array}$$

and thus, up to Z^7,

$$\begin{aligned} A^{(1)}_2(Z) &= Z^3 + \frac{Z^2}{1-Z} = Z^3 + \sum_{n=0}^{K-4} Z^{2+n} = Z^2 + 2Z^3 + Z^4 + Z^5 + Z^6 + Z^7 + \cdots + Z^n + \cdots \\ A^{(2)}_4(Z) &= Z^6 + \frac{2Z^5}{1-Z} + \frac{Z^4}{(1-Z)^2} = Z^6 + 2\sum_{n=0}^{K-7} Z^{5+n} + \sum_{n=0}^{K-8}(n+1)Z^{4+n} \\ &= Z^4 + 4Z^5 + 6Z^6 + 6Z^7 + \cdots + (n-1)Z^n + \cdots . \end{aligned}$$

The multiple turbo code, as shown in Figure 16.2, contains 3 encoders, and it is assumed that the interleavers are uniformly distributed, the block size K is large, and the code uses the same constituent encoders. Assume that a particular input sequence of weight w enters the first encoder, generating the parity weight enumerator $A^{PC}_w(Z)$. Then, by the definition of the uniform interleaver, the second *and* third encoders will generate any of the weights in $A^{PC}_w(Z)$ with equal probability. The codeword CWEF of this $(4K, K-2)$ terminated multiple turbo code is given by

$$\begin{aligned} A^{PC}_w(Z) &= \left[\sum_{h_1=1}^{h_{max}} c[h_1,w]A^{(h_1)}_w(Z)\right] \left[\sum_{h_2=1}^{h_{max}} c[h_2,w]\binom{K}{w}^{-1} A^{(h_2)}_w(Z)\right] \left[\sum_{h_3=1}^{h_{max}} c[h_3,w]\binom{K}{w}^{-1} A^{(h_3)}_w(Z)\right] \\ &= \sum_{h_1=1}^{h_{max}} \sum_{h_2=1}^{h_{max}} \sum_{h_3=1}^{h_{max}} \binom{K}{w}^{-2} c[h_1,w]\ c[h_2,w]\ c[h_3,w]\ A^{(h_1)}_w(Z)\ A^{(h_2)}_w(Z)\ A^{(h_3)}_w(Z) \quad , \end{aligned}$$

where h_{max} is the maximum number of error events for the particular choice of w and $c[h,w] = \binom{K-h+w}{w}$. With $K \gg h$ and $K \gg w$, $c[h,w] \approx \binom{K}{h} \approx \frac{K^h}{h!}$, and $h_{max} = \lfloor \frac{w}{2} \rfloor$. These approximations, along with keeping only the highest power of K, i.e., the term corresponding to $h_1 = h_2 = h_3 = h_{max}$, result in the codeword CWEF

$$A_w^{PC}(Z) \approx \frac{(w!)^2}{(h_{max}!)^3} K^{(3h_{max}-2w)} \left[A_w^{(h_{max})}(Z) \right]^3$$

and the bit CWEF

$$B_w^{PC}(Z) = \frac{w}{K} A_w^{PC}(Z) \approx \frac{w\ (w!)^2}{(h_{max}!)^3} K^{(3h_{max}-2w-1)} \left[A_w^{(h_{max})}(Z) \right]^3 \quad .$$

Then, for $w < 6$, the approximate IRWEF's for this PCCC are

$$A^{PC}(W,Z) \approx \sum_{w=2}^{5} W^w A_w^{PC}(Z) \ \text{ and } \ B^{PC}(W,Z) \approx \sum_{w=2}^{5} W^w B_w^{PC}(Z),$$

and the WEF's are $A^{PC}(X) = A^{PC}(X,X)$ and $B^{PC}(X) = B^{PC}(X,X)$. From the above,

$$\begin{aligned} \left[A_2^{(1)}(Z) \right]^3 &= Z^9 + \frac{3Z^8}{1-Z} + \frac{3Z^7}{(1-Z)^2} + \frac{Z^6}{(1-Z)^3} \\ &= Z^6 + 6Z^7 + 15Z^8 + 23Z^9 + 30Z^{10} + 39Z^{11} + \cdots + \left(\frac{n^2-3n-10}{2} \right) Z^n + \cdots \end{aligned}$$

and

$$\begin{aligned} \left[A_4^{(2)}(Z) \right]^3 &= Z^{18} + \frac{6Z^{17}}{1-Z} + \frac{15Z^{16}}{(1-Z)^2} + \frac{20Z^{15}}{(1-Z)^3} + \frac{16Z^{14}}{(1-Z)^4} + \frac{6Z^{13}}{(1-Z)^5} + \frac{Z^{12}}{(1-Z)^6} \\ &= Z^{12} + 12Z^{13} + 66Z^{14} + 226Z^{15} + 561Z^{16} + 1128Z^{17} + 1995Z^{18} + 3258Z^{19} + \\ &\quad 5028Z^{20} + \cdots + \left(\frac{-21720 - 7046n + 3015n^2 - 155n^3 - 15n^4 + n^5}{120} \right) Z^n + \cdots . \end{aligned}$$

(a) Using the above, the approximate CWEF's up to Z^{14} are

$$\begin{aligned} A_2^{PC}(Z) &\approx \tfrac{4}{K} \left[A_2^{(1)}(Z) \right]^3 = \tfrac{4}{K} Z^6 + \tfrac{24}{K} Z^7 + \tfrac{60}{K} Z^8 + \tfrac{92}{K} Z^9 + \tfrac{120}{K} Z^{10} + \tfrac{156}{K} Z^{11} + \\ &\qquad \tfrac{196}{K} Z^{12} + \tfrac{240}{K} Z^{13} + \tfrac{288}{K} Z^{14} + \cdots + 2 \left(\tfrac{n^2-3n-10}{K} \right) Z^n + \cdots \\ A_4^{PC}(Z) &\approx \tfrac{72}{K^2} \left[A_4^{(2)}(Z) \right]^3 \approx \tfrac{72}{K^2} Z^{12} + \tfrac{864}{K^2} Z^{13} + \tfrac{4752}{K^2} Z^{14} + \cdots \\ A_3^{PC}(Z) &= A_5^{PC}(Z) = 0 \\ B_2^{PC}(Z) &= \tfrac{2}{K} \left[A_2^{PC}(Z) \right] \approx \tfrac{8}{K^2} Z^6 + \tfrac{48}{K^2} Z^7 + \tfrac{120}{K^2} Z^8 + \tfrac{184}{K^2} Z^9 + \tfrac{240}{K^2} Z^{10} + \tfrac{312}{K^2} Z^{11} + \\ &\qquad \tfrac{392}{K^2} Z^{12} + \tfrac{480}{K^2} Z^{13} + \tfrac{576}{K^2} Z^{14} + \cdots + 4 \left(\tfrac{n^2-3n-10}{K^2} \right) Z^n + \cdots \\ B_4^{PC}(Z) &= \tfrac{4}{K} \left[A_4^{PC}(Z) \right] \approx \tfrac{288}{K^3} Z^{12} + \tfrac{3456}{K^3} Z^{13} + \tfrac{19008}{K^3} Z^{14} + \cdots \\ B_3^{PC}(Z) &= B_5^{PC}(Z) = 0 \end{aligned}$$

(b) Using the above, the approximate IRWEF's up to W^5 and Z^{14} are

$$\begin{aligned} A^{PC}(W,Z) &\approx W^2\left[\tfrac{4}{K}Z^6 + \tfrac{24}{K}Z^7 + \tfrac{60}{K}Z^8 + \tfrac{92}{K}Z^9 + \tfrac{120}{K}Z^{10} + \tfrac{156}{K}Z^{11} + \right. \\ &\qquad \left. \tfrac{196}{K}Z^{12} + \tfrac{240}{K}Z^{13} + \tfrac{288}{K}Z^{14} + \cdots + 2\left(\tfrac{n^2-3n-10}{K}\right)Z^n + \cdots\right] + \\ &\quad W^4\left[\tfrac{72}{K^2}Z^{12} + \tfrac{864}{K^2}Z^{13} + \tfrac{4752}{K^2}Z^{14} + \cdots\right] \end{aligned}$$

and

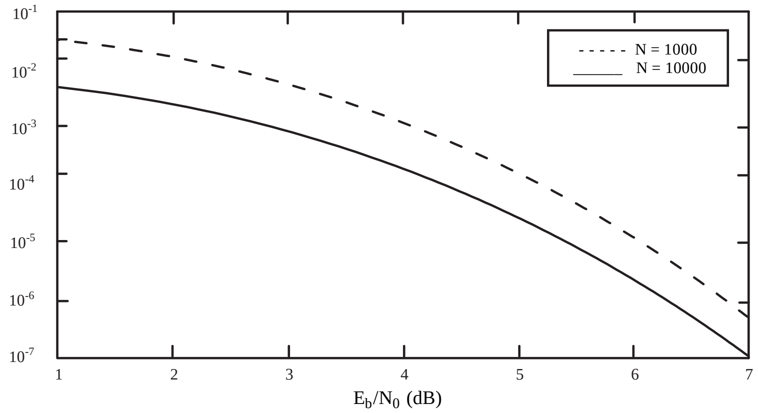
$$\begin{aligned} B^{PC}(W,Z) &\approx W^2\left[\tfrac{8}{K^2}Z^6 + \tfrac{48}{K^2}Z^7 + \tfrac{120}{K^2}Z^8 + \tfrac{184}{K^2}Z^9 + \tfrac{240}{K^2}Z^{10} + \tfrac{312}{K^2}Z^{11} + \right. \\ &\qquad \left. \tfrac{392}{K^2}Z^{12} + \tfrac{480}{K^2}Z^{13} + \tfrac{576}{K^2}Z^{14} + \cdots + 4\left(\tfrac{n^2-3n-10}{K^2}\right)Z^n + \cdots\right] + \\ &\quad W^4\left[\tfrac{288}{K^3}Z^{12} + \tfrac{3456}{K^3}Z^{13} + \tfrac{19008}{K^3}Z^{14} + \cdots\right] \end{aligned}$$

(c) Using the above, the approximate WEF's up to X^{14}, neglecting any higher power of K terms, are

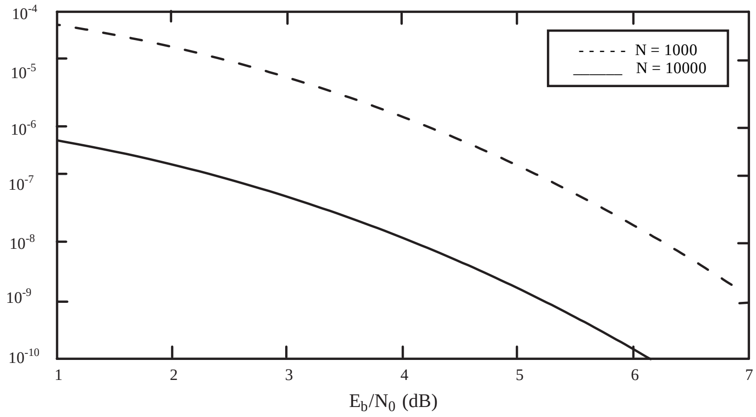
$$A^{PC}(X) \approx \frac{4}{K}X^8 + \frac{24}{K}X^9 + \frac{60}{K}X^{10} + \frac{92}{K}X^{11} + \frac{120}{K}X^{12} + \frac{156}{K}X^{13} + \frac{196}{K}X^{14} + \cdots$$

and $$B^{PC}(X) \approx \frac{8}{K^2}X^8 + \frac{48}{K^2}X^9 + \frac{120}{K^2}X^{10} + \frac{184}{K^2}X^{11} + \frac{240}{K^2}X^{12} + \frac{312}{K^2}X^{13} + \frac{392}{K^2}X^{14} + \cdots$$

(d) The union bounds on the BER and WER for $K = 10^3$ and $K = 10^4$, assuming a binary input, unquantized output AWGN channel are shown below. The plots were created using the loose bounds $WER \leq A^{PC}(X)\Big|_{X=e^{-\frac{R\,E_b}{N_0}}}$ and $BER \leq B^{PC}(X)\Big|_{X=e^{-\frac{R\,E_b}{N_0}}}$ where $R = 1/4$ is the code rate and $\frac{E_b}{N_0}$ is the SNR.



(a) Word Error Rate



(b) Bit Error Rate

16.15 (a) $\begin{bmatrix} 1 & \frac{1}{1+D} \end{bmatrix}$

i. Weight 2
Minimum parity weight generating information sequence $= 1 + D$.
Corresponding parity weight $= 1$.
In a PCCC (rate 1/3) we therefore have (assuming a similar input after interleaving):
Information weight $= 2$; Parity weight $= 1 + 1 = 2$; Total weight $= 4$.

ii. Weight 3
For this encoder a weight 3 input does not terminate the encoder and hence is not possible.

(b) $\begin{bmatrix} 1 & \frac{1+D^2}{1+D+D^2} \end{bmatrix}$

i. Weight 2
Minimum parity weight generating information sequence $= 1 + D^3$.
Corresponding parity weight $= 4$.
In a PCCC we therefore have:
Information weight $= 2$; Parity weight $= 4 + 4 = 8$; Total weight $= 10$.

ii. Weight 3
Minimum parity weight generating information sequence $= 1 + D + D^2$.
Corresponding parity weight $= 2$.
In a PCCC we therefore have:
Information weight $= 3$; Parity weight $= 2 + 2 = 4$; Total weight $= 7$.

(c) $\begin{bmatrix} 1 & \frac{1+D^2+D^3}{1+D+D^3} \end{bmatrix}$

i. Weight 2
Minimum parity weight generating information sequence $= 1 + D^7$.
Corresponding parity weight $= 6$.
In a PCCC we therefore have:
Information weight $= 2$; Parity weight $= 6 + 6 = 12$; Total weight $= 14$.

ii. Weight 3
Minimum parity weight generating information sequence $= 1 + D + D^3$.
Corresponding parity weight $= 4$.
In a PCCC we therefore have:
Information weight $= 3$; Parity weight $= 4 + 4 = 8$; Total weight $= 11$.

(d) $\left[1 \quad \frac{1+D+D^2+D^4}{1+D^3+D^4}\right]$

i. Weight 2
Minimum parity weight generating information sequence $= 1 + D^{15}$.
Corresponding parity weight $= 10$.
In a PCCC we therefore have:
Information weight $= 2$; Parity weight $= 10 + 10 = 20$; Total weight $= 22$.

ii. Weight 3
Minimum parity weight generating information sequence $= 1 + D^3 + D^4$.
Corresponding parity weight $= 4$.
In a PCCC we therefore have:
Information weight $= 3$; Parity weight $= 4 + 4 = 8$; Total weight $= 11$.

(e) $\left[1 \quad \frac{1+D^4}{1+D+D^2+D^3+D^4}\right]$

i. Weight 2
Minimum parity weight generating information sequence $= 1 + D^5$.
Corresponding parity weight $= 4$.
In a PCCC we therefore have:
Information weight $= 2$; Parity weight $= 4 + 4 = 8$; Total weight $= 10$.

ii. Weight 3
For this encoder a weight 3 input does not terminate the encoder and hence is not possible.

In all cases the input weight two sequence gives the free distance codeword for large K.

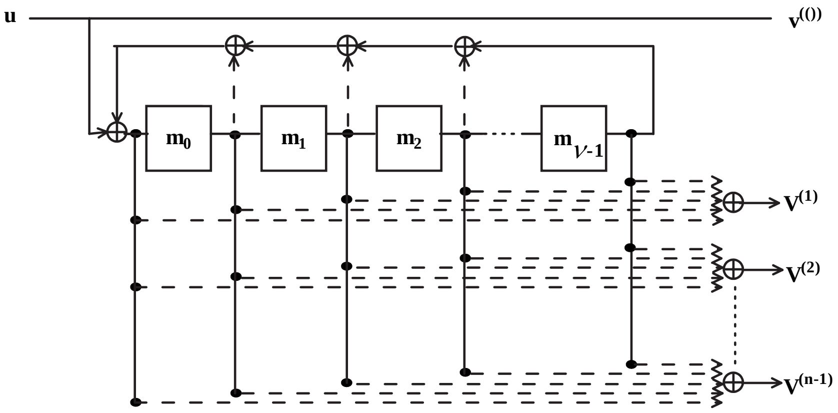
16.16 For a systematic feedforward encoder, for input weight w, the single error event for input weight 1 can occur w times. Therefore h_{max}, the largest number of error events associated with a weight w input sequence, is equal to w. That is, the maximum number of error events produced by a weight w input sequence occurs by repeating the single error event for input weight 1 w times. Thus,

$$A_w^{(w)}(Z) = [A_1^{(1)}(Z)]^w.$$

This is not true for feedback encoders. Feedback encoders require at least a weight 2 input sequence to terminate. Thus, for an input sequence of weight $2w, h_{max} = w$, i.e., we have a maximum of w error events. This occurs when an error event caused by a weight 2 input sequence is repeated w times (for a total input weight of $2w$).

Therefore

$$A_{2w}{}^{(w)}(Z) = [A_Z{}^{(1)}(Z)]^w.$$



16.19 An $(n, 1, v)$ systematic feedback encoder can be realized by the following diagram:

In the figure, the dashed lines indicate potential connections that depend on the encoder realization. It can be seen from the encoder structure that the register contents are updated as

$$m_{i,t} = m_{i-1,t-1} \qquad , i = 1, 2, \ldots, v-1$$

and

$$m_{0,t} = m_{v-1,t-1} + u_t + \sum_{i=0}^{v-2} a_i m_{i,t-1},$$

where t is the time index, u_t represents the input bit at time t, and the coefficients a_i depend on the particular encoder realization. When the encoder is in state $S_{2^{v-1}} = (0\,0\ldots 1)$ at time $t-1$, it follows from the given relations that

$$m_{i,t} = m_{i-1,t-1} = 0, \qquad i = 1, 2, \ldots, v-1$$

and

$$m_{0,t} = m_{v-1,t-1} + u_t + \sum_{i=0}^{v-2} a_i m_{i,t-1} = 1 + u_t.$$

Thus if the input bit $u_t = 1$, the first memory position at time t is also 0, and the encoder is in the all-zero state.

16.20 For the primitive encoder D with $G_p(D) = \begin{bmatrix} 1 & \frac{D^4+D^2+D+1}{D^4+D^3+1} \end{bmatrix}$, the shortest terminating weight 2 input sequence is

$$u(D) = 1 + D^{2^4-1} = 1 + D^{15},$$

which generates the parity sequence

$$\begin{aligned} v(D) &= (1+D^3+D^4+D^6+D^8+D^9+D^{10}+D^{11})(D^4+D^2+D+1) \\ &= 1+D+D^2+D^3+D^4+D^8+D^{11}+D^{12}+D^{14}+D^{15}. \end{aligned}$$

Thus

$$Z_{min} = 10$$

and

$$d_{eff} = 2 + 2\,Z_{min} = 2 + 2 \times 10 = 22.$$

For the nonprimitive encoder E with $G_{np}(D) = \left[1 \quad \frac{D^4+1}{D^4+D^3+D^2+D+1}\right]$, the shortest terminating weight 2 input sequence is $u(D) = 1 + D^5$, which generates the parity sequence

$$v(D) = (D+1)(D^4+1) = 1 + D + D^4 + D^5.$$

Thus $Z_{min} = 4$ and $d_{eff} = 2 + 2Z_{min} = 10$.

Chapter 20

20.1 If an (n, k) code $\mathcal{C}$ is designed to correct all the bursts of length l or less and simultaneously to detect all the bursts of length d or less with $d \geq l$, then no burst of length $l + d$ or less can be a codeword. Suppose there is a burst $\boldsymbol{x}$ of length $l + d$ or less that is a codeword in $\mathcal{C}$. We can decompose this burst $\boldsymbol{x}$ into two bursts $\boldsymbol{y}$ and $\boldsymbol{z}$ such that: (1) $\boldsymbol{x} = \boldsymbol{y} + \boldsymbol{z}$; (2) the length of $\boldsymbol{y}$ is l or less and the length of $\boldsymbol{z}$ is d or less. Since the code is designed to correct all the bursts of length l or less, $\boldsymbol{y}$ must be a coset leader in a standard array for the code. Since $\boldsymbol{y} + \boldsymbol{z} = \boldsymbol{x}$ is codeword, then $\boldsymbol{z}$ must be in the same coset as $\boldsymbol{y}$. As a results, $\boldsymbol{z}$ has the same syndrome as $\boldsymbol{y}$. In this case, if $\boldsymbol{z}$ occurs as an error burst during the transmission of a codeword in $\mathcal{C}$, then $\boldsymbol{y}$ will be taken as the error burst for correction. This will result in an incorrect decoding and hence the decoder will fail to detect $\boldsymbol{z}$ which contradicts to the fact that the code is designed to correct all the bursts of lengths l or less and simultaneously to detect all the bursts of length d or less with $d \geq l$. Therefore, a burst of length $l + d$ or less can not be a codeword. Then it follows from Theorem 20.2 that $n - k \geq l + d$.

20.2 An error-trapping decoder is shown in Figure P20.2.

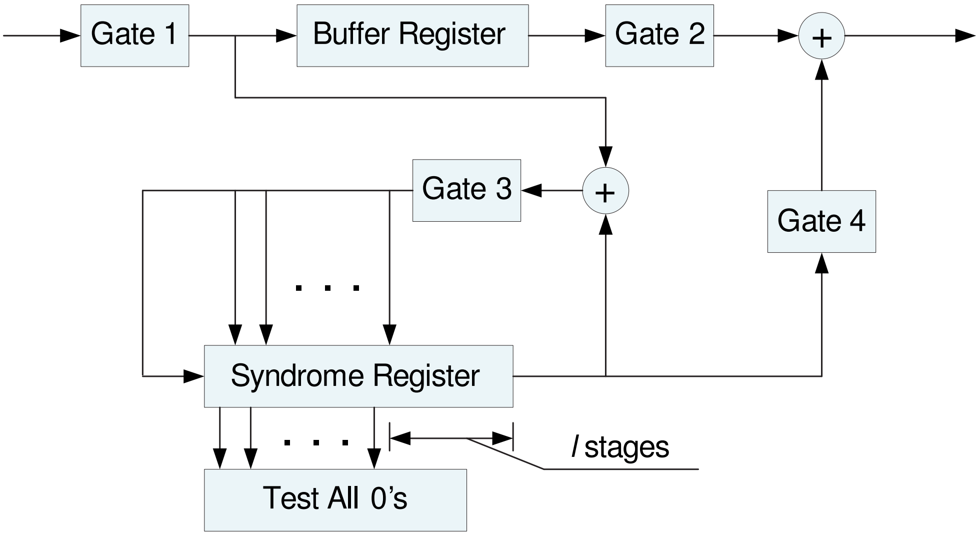


Figure P20.2 An error-trapping decoder.

The decoding operation is given below:

Step 1. The received polynomial $\boldsymbol{r}(x)$ is shifted into the buffer and syndrome registers simultaneously with Gates 1 and 3 turned on and all the other gates turned off.

Step 2. As soon as the entire $\boldsymbol{r}(x)$ has been shifted into the syndrome register, the contents of the syndrome form the syndrome $\boldsymbol{S}^{(n-k)}(x)$ of $\boldsymbol{r}^{(n-k)}(x)$. If the $n-k-l$ leftmost stages of the syndrome register contain all zeros, the error burst is confined to the positions X^{n-l}, $\ldots$, $Xn-1$. Gate 2 and Gate 4 are activated. The received information digits are read out of the buffer register and connected by the error digits shifted out from the syndrome register. If $n-k-l$ leftmost stages of the syndrome register does not contain all zeros, go to step 3.

Step 3. The syndrome register starts to shift with Gate 3 on. As soon as its $n-k-l$ leftmost stages contain only zeros, its l rightmost stages contain the burst-error pattern. The error correction begins. there are three cases to be considered.

Step 4. If the $n-k-l$ leftmost stages of the syndrome register contains all zeros after ith shift $0 < i \leq 2k-n$ (Assume $2k-n \geq 0$, otherwise, no this step), the error burst is confined to positions $X^{n-i-1-l}$, $\ldots$, X^{n-i-1}. In this event, Gate 2 is first activated and the i high position information digits are shifted out. Then Gate 4 is activated, the rest information digits are read out and corrected by the error digit shifted out from the syndrome register.

Step 5. If the $n-k-l$ leftmost stages of the syndrome register contains all zeros after the ith shift $k \leq i \leq n-l$, the errors of the burst $\boldsymbol{e}(x)$ are confined to the parity-check positions of $\boldsymbol{r}(x)$. In this event, the k received information digits in the buffer are error free. Gate 2 is activated and the k error-free information digits in the buffer are shifted out to the data sink.

Step 6. if the $n-k-l$ leftmost stages of the syndrome register contains all zeros after $(n-l+i)$th shift $0 < i < l$, the error burst is confined to positions X^{n-i}, $\ldots$, X^{n-1}, X^0, X^{l-i-1}. In this event, the $l-i$ digits contained in the $l-i$ rightmost stages of the syndrome register match the errors at the parity-check positions of $\boldsymbol{r}(X)$, and the i digits contained int the next i stages of the syndrome register match the errors at the positions X^{n-i}, $\ldots$, X^{n-1} of $\boldsymbol{r}(X)$. At this instant, a clock starts to count from $(n-l+i+1)$. The syndrome register is then shifted with Gate 3 turned off. As soon as the clock has counted up to n, the i rightmost digits in the syndrome register match the errors at the positions X^{n-i}, $\ldots$, X^{n-l}, X^{n-1} of $\boldsymbol{r}(X)$. Gate 4 and Gate 2 are then activated. The received information digits are read out of the buffer register and corrected by the error digits shifted out from the syndrome register.

If the $n-k-l$ stages of the syndrome never contain all zeros after all the steps above, an uncorrectable burst of errors has been detected.

20.4 The generator polynomial of the desired Fire code is

$$\boldsymbol{g}(X) = (X^{2l-1}+1)\boldsymbol{p}(X)$$

Since the code is designed to correct all the bursts of length 4 or less, $l=4$. Hence

$$\boldsymbol{g}(X) = (X^7+1)(1+X+X^4) = 1+X+X^4+X^7+X^8+X^{11}.$$

Since $\boldsymbol{p}(X)$ is a primitive polynomial of degree 4, its period ρ is $2^4-1=15$. Hence the length of the code is $n = LCM(7,15) = 105$. Since the degree of the generator polynomial of the code is 11 which is the number of parity check digits of the code, the code is a $(105,94)$ Fire code. The decoder of this code is shown in Figure P20.4.

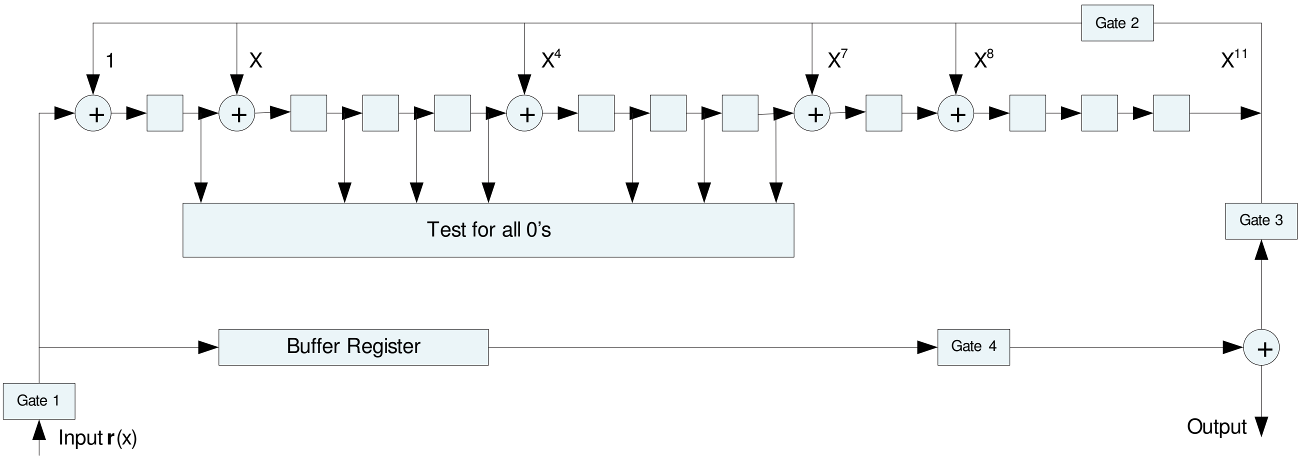


Figure P20.4 A decoder for the $(105,94)$ Fire code.

20.5 The high-speed decoder for the $(105, 94)$ Fire code designed in Problem 20.4 is shown in Figure P20.5.

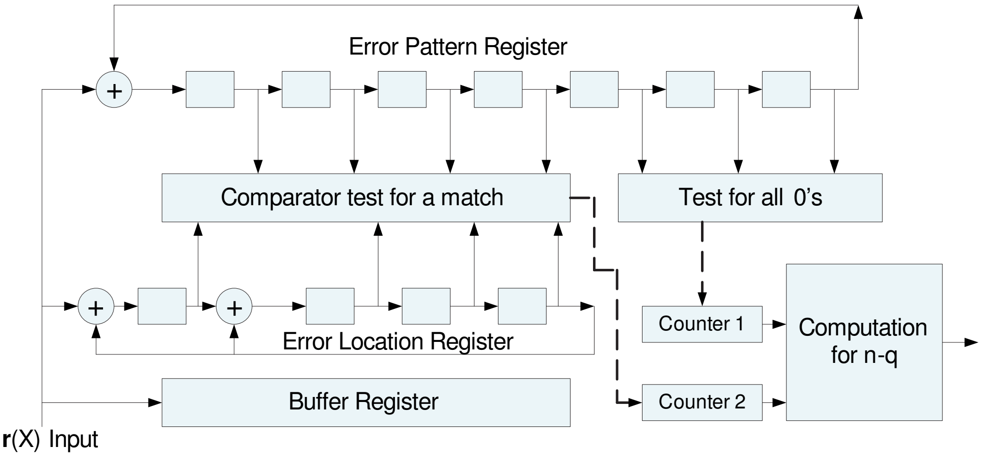


Figure P20.5 A high-speed decoder for the $(105, 94)$ Fire code.

20.6 We choose the second code given in Table 20.3 which is a $(15, 9)$ code and capable of correcting any burst of length 3 or less. The burst-error-correcting efficiency $z = 1$. The generator polynomial of this code is $\boldsymbol{g}(X) = 1 + X^3 + X^4 + X^5 + X^6$. Suppose we interleave this code by a degree $\lambda = 17$. This results in a $(255, 153)$ cyclic code that is capable of correcting any single burst of length 51 or less and has burst-error-correcting efficiency $z = 1$. The generator of this code is

$$\boldsymbol{g}'(X) = \boldsymbol{g}(X^{17}) = 1 + X^{51} + X^{68} + X^{85} + X^{102}.$$

A decoder for this code can be implemented with a de-interleaver and the decoder for the $(15, 9)$ code as shown in Figure P20.6. First the received sequence is de-interleaved and arranged as a 17×15 array. Then each row of the array is decoded based on the base $(15, 9)$ code.

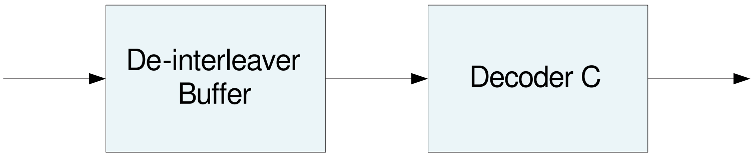


Figure P20.6 A decoder for the $(255, 153)$ burst-error-correcting code designed above.

20.7 A codeword in the interleaved code $\mathcal{C}_\lambda^l$ is obtained by interleaving l codewords from the (n, k) base code $\mathcal{C}$. Let $\boldsymbol{v}_1(X)$, $\boldsymbol{v}_2(X)$, $\ldots$, $\boldsymbol{v}_l(X)$ be l codewords in $\mathcal{C}$. Then the codeword in $\mathcal{C}_\lambda^l$

obtained by interleaving these l codewords in $\mathcal{C}$ in polynomial form is

$$\boldsymbol{v}(X) = \boldsymbol{v}_1(X^l) + X\boldsymbol{v}_2(X^l) + X^2\boldsymbol{v}_3(X^l) + \ldots + X^{l-1}\boldsymbol{v}_l(X^l).$$

Since $\boldsymbol{v}_i(X)$ is divisible by $\boldsymbol{g}(X)$ for $1 \leq i \leq l$, $\boldsymbol{v}_i(X^l)$ is divisible by $\boldsymbol{g}(X^l)$. Therefore $\boldsymbol{v}(X)$ is divisible by $\boldsymbol{g}(X^l)$. The degree of $\boldsymbol{g}(X^l)$ is $(n-k)l$. Since $\boldsymbol{g}(X^l)$ is a factor of $X^{ln}+1$, $\boldsymbol{g}(X^l)$ generates a (ln, lk) cyclic code.

20.8 In order to show that the Burton code is capable of correcting all phased bursts confined to a single subblock of m digits, it is necessary and sufficient to prove that no two such bursts are in the same coset of a standard array for the code. Let $X^{mi}\mathbf{A}(X)$ and $X^{mj}\mathbf{B}(X)$ be the polynomial representations of two bursts of length l_1 and l_2 with $l_1 \leq m$ and $l_2 \leq m$ confined to ith and jth subblocks $(0 \leq i \leq \sigma, 0 \leq j \leq \sigma)$, respectively, where

$$\mathbf{A}(X) = 1 + a_1X + \ldots + a_{l_1-2}X^{l_1-2} + X^{l_1-1},$$

and

$$\mathbf{B}(X) = 1 + b_1X + \ldots + b_{l_2-2}X^{l_2-2} + X^{l_2-1}.$$

Suppose $X^{mi}A(X)$ and $X^{mj}B(X)$ are in the same coset. Then $\mathbf{V}(X) = X^{mi}\mathbf{A}(X) + X^{mj}\mathbf{B}(X)$ must be a code polynomial and divisible by the generator polynomial $\boldsymbol{g}(X) = (X^m+1)\boldsymbol{p}(X)$. Assume $mj \geq mi$, then $mj - mi = qm$ and

$$\mathbf{V}(X) \;\; = \;\; X^{mi}(\mathbf{A}(X) + \mathbf{B}(X)) + X^{mi}\mathbf{B}(X)(X^{qm}+1).$$

Since $X^m - 1$ is a factor of the generator $\boldsymbol{g}(X)$, $\mathbf{V}(X)$ must be divisible by $X^m - 1$. Note that $X^{qm}+1$ is divisible by X^m+1, and X^{mi} and X^m+1 are relatively prime. Since $\mathbf{V}(X)$ and $X^{mi}\mathbf{B}(X)(X^{qm}+1)$ are divisible by X^m+1, $\mathbf{A}(X)+\mathbf{B}(X)$ must be divisible by X^m+1. However both degrees l_1 and l_2 of $\mathbf{A}(X)$ and $\mathbf{B}(X)$ are less than m, the degree of $\mathbf{A}(X)+\mathbf{B}(X)$ is less than m. Hence $\mathbf{A}(X)+\mathbf{B}(X)$ is not divisible by X^m+1. For $\mathbf{V}(X)$ to be divisible by X^m+1, $\mathbf{A}(X)$ and $\mathbf{B}(X)$ must be identical, i.e., $\mathbf{A}(X) = \mathbf{B}(X)$. Therefore,

$$\mathbf{V}(X) = X^{mi}\mathbf{B}(X)(X^{qm}+1).$$

Since the degree of $\mathbf{B}(X)$ is less than m, $\mathbf{B}(X)$ and $\boldsymbol{p}(X)$ must be relatively prime. Also X^{mi} and $\boldsymbol{p}(X)$ are relatively prime. Since $\mathbf{V}(X)$ is assumed to be a code polynomial, $X^{qm}+1$ must be divisible by both $\boldsymbol{p}(X)$ and X^m-1. This implies that $X^{qm}+1$ is divisible by $(X^m+1)\boldsymbol{p}(X)$ and qm must be a multiple of $n=\sigma m$. This is not possible, since $q=j-i$ is less than σ. Therefore $\mathbf{V}(X)$ can not be a code polynomial and the bursts $X^{mi}\mathbf{A}(X)$ and $X^{mi}\mathbf{B}(X)$ can not be in the same coset. Consequently, all the phased bursts confined to a single subblock of m digits are in different cosets of a standard array for the Burton code generated by $(X^m+1)\boldsymbol{p}(X)$ and they are correctable.

20.9 Choose $\boldsymbol{p}(X)=1+X^2+X^5$ which is a primitive polynomial with period $\rho=2^5-1=31$. Then generator polynomial of the Burton code $\mathcal{C}$ with $m=5$ is

$$\boldsymbol{g}(X)=(X^m+1)\boldsymbol{p}(X)=1+X^2+X^7+X^{10}.$$

The length of the code is $n=LCM(31,5)=155$. Hence the code is a $(155,145)$ code that is capable of correcting any phased burst confined to a single subblock of 5 digits. If the code is interleaved to a degree $\lambda=6$, we obtain a $(930,870)$ code $\mathcal{C}^6$ generated by $\boldsymbol{g}(X^6)=1+X^{12}+X^{42}+X^{60}$. This code is capable of correcting any burst of length $5\times 5+1=26$ or less.

20.10 From Table 9.3, code $(164,153)$ has burst-correcting-capability $l=4$. If it is interleaved to degree $\lambda=6$, then $\lambda n=6\times 164=984$, $\lambda k=6\times 153=918$, and $\lambda l=6\times 4=24$. The interleaved code is a $(984,918)$ code with burst-error-correcting capability 24.

The interleaved Burton code of Problem 20.9 is a $(930,870)$ code with burst-error-correcting capability 26. The burst-error-correcting efficiency of the $(984,918)$ code is

$$z=\frac{2\lambda l}{\lambda n-\lambda k}=\frac{48}{984-918}=\frac{8}{11}.$$

The efficiency of the interleave Burton code of Problem 20.9 is

$$z'=\frac{2[(\lambda-1)m+1]}{2\lambda m}=\frac{52}{60}=\frac{13}{15}.$$

Therefore, $z'\geq z$. The interleaved Burton code is more powerful and efficient.

20.11 The $(15, 7)$ BCH code has random error-correcting capability 2. Interleaving this code to a degree 7, we obtain a $(105, 49)$ cyclic code that is capable of correcting any combination of two random bursts, each of length 7 or less. Of course, it is capable of correcting any single burst of length 14 or less. In decoding, a received sequence is de-interleaved and arranged into a 7×15 array. Each row of the array is decoded based on the $(15, 7)$ BCH code.

20.12 If each symbol of the $(31, 15)$ RS code over GF(2^5) is replaced by its corresponding 5-bit byte, we obtain a $(155, 75)$ binary code. Since the $(31, 15)$ RS code is capable of correcting 8 or fewer random symbol errors, the binary $(155, 75)$ code is capable of correcting: (1) any single burst of length $(8 - 1) \times 5 + 1 = 36$ or less; or (2) correcting any combination random bursts that result in 8 or fewer random symbol errors for the $(31, 15)$ RS code.

20.13 From Problem 20.4, the generator polynomial

$$\boldsymbol{g}(X) = 1 + X + X^4 + X^7 + X^8 + X^{11}$$

generates a $(105, 94)$ Fire code. If it is shortened by deleting the 15 high-order message digits, it becomes a $(90, 79)$ code.

Dividing $X^{n-k+15} = X^{26}$ by $\boldsymbol{g}(X)$, we obtain a remainder $\boldsymbol{\rho}(X) = X^{10}+X^8+X^5+X^3+X$. Then a decoder for the $(105, 94)$ shortened Fire code is shown in Figure P20.13

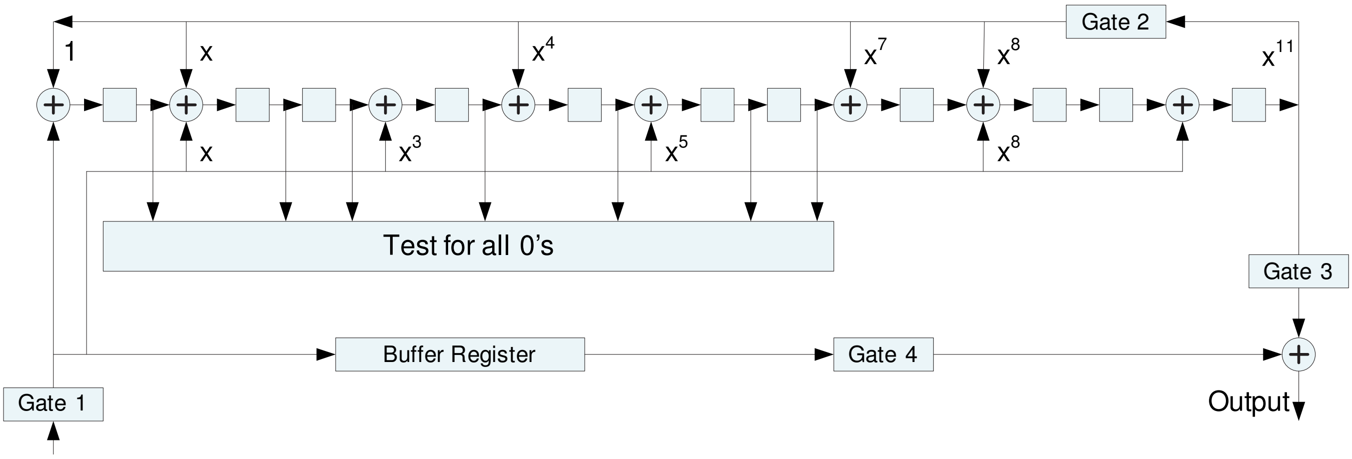


Figure P20.13 A decoder for the $(90, 79)$ Fire code.

20.14 Let α be a primitive element of the Galois field GF(2^6). The order of α is $2^6 - 1 = 63$ and the minimal polynomial of α is

$$\Phi(X) = 1 + X + X^6.$$

Since $63 = 7 \times 9$, we can factor $X^{63} + 1$ as follows:

$$X^{63} + 1 = (X^7 + 1)(1 + X^7 + X^{14} + X^{21} + X^{28} + X^{35} + X^{42} + X^{49} + X^{56}).$$

The code generated by the polynomial

$$\boldsymbol{g}_1(X) = (X^7 + 1)(1 + X + X^6)$$

is a Fire code of length 63 which is capable of correcting any single error burst of length 4 or less. Let $\boldsymbol{g}_2(X)$ be the generator polynomial of the double-error-correcting BCH code of length 63. From Table 6.4, we find that

$$\boldsymbol{g}_2(X) = (1 + X + X^6)(1 + X + X^2 + X^4 + X^6).$$

The least common multiple of $\boldsymbol{g}_1(X)$ and $\boldsymbol{g}_2(X)$ is

$$\boldsymbol{g}(X) = (1 + X^7)(1 + X + X^6)(1 + X + X^2 + X^4 + X^6).$$

Hence, $\boldsymbol{g}(X)$ generates a $(63, 44)$ cyclic code which is a modified Fire code and is capable of correcting any single error burst of length 4 or less as well as any combination of two or fewer random errors.