Two matrices can be added if they have the same number of rows and the same number of columns. To add two $k \times n$ matrices $\mathbb{A} = [a_{ij}]$ and $\mathbb{B} = [b_{ij}]$, we simply add their corresponding entries a_{ij} and b_{ij} as follows:

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}].$$

Hence, the resultant matrix is also a $k \times n$ matrix. Two matrices can be multiplied provided that the number of columns in the first matrix is equal to the number of rows in the second matrix. Multiplying a $k \times n$ matrix $\mathbb{A} = [a_{ij}]$ by an $n \times l$ matrix $\mathbb{B} = [b_{ij}]$, we obtain the product

$$\mathbb{C} = \mathbb{A} \times \mathbb{B} = [c_{ij}].$$

In the resultant $k \times l$ matrix the entry c_{ij} is equal to the inner product of the ith row $\mathbb{a}_i$ in $\mathbb{A}$ and the jth column $\mathbb{b}_j$ in $\mathbb{B}$; that is,

$$c_{ij} = \mathbb{a}_i \cdot \mathbb{b}_j = \sum_{t=0}^{n-1} a_{it} b_{tj}.$$

Let $\mathbb{G}$ be a $k \times n$ matrix over $GF(2)$. The *transpose* of $\mathbb{G}$, denoted by $\mathbb{G}^T$, is an $n \times k$ matrix whose rows are columns of $\mathbb{G}$ and whose columns are rows of $\mathbb{G}$. A $k \times k$ matrix is called an *identity* matrix if it has 1's on the main diagonal and 0's elsewhere. This matrix is usually denoted by $\mathbb{I}_k$. A *submatrix* of a matrix $\mathbb{G}$ is a matrix that is obtained by striking out given rows or columns of $\mathbb{G}$.

It is straightforward to generalize the concepts and results presented in this section to matrices with entries from $GF(q)$ with q as a power of a prime.

PROBLEMS

2.1 Construct the group under modulo-6 addition.

2.2 Construct the group under modulo-3 multiplication.

2.3 Let m be a positive integer. If m is not a prime, prove that the set $\{1, 2, \cdots, m-1\}$ is not a group under modulo-m multiplication.

2.4 Construct the prime field $GF(11)$ with modulo-11 addition and multiplication. Find all the primitive elements, and determine the orders of other elements.

2.5 Let m be a positive integer. If m is not prime, prove that the set $\{0, 1, 2, \cdots, m-1\}$ is not a field under modulo-m addition and multiplication.

2.6 Consider the integer group $G = \{0, 1, 2, \cdots, 31\}$ under modulo-32 addition. Show that $H = \{0, 4, 8, 12, 16, 20, 24, 28\}$ forms a subgroup of G. Decompose G into cosets with respect to H (or modulo H).

2.7 Let λ be the characteristic of a Galois field $GF(q)$. Let 1 be the unit element of $GF(q)$. Show that the sums

$$1, \sum_{i=1}^{2} 1, \sum_{i=1}^{3} 1, \cdots, \sum_{i=1}^{\lambda-1} 1, \sum_{i=1}^{\lambda} 1 = 0$$

form a subfield of $GF(q)$.

2.8 Prove that every finite field has a primitive element.

2.9 Solve the following simultaneous equations of X, Y, Z, and W with modulo-2 arithmetic:

$$\begin{aligned} X + Y \quad\quad + W &= 1, \\ X \quad + Z + W &= 0, \\ X + Y + Z + W &= 1, \\ Y + Z + W &= 0. \end{aligned}$$

2.10 Show that $X^5 + X^3 + 1$ is irreducible over $GF(2)$.

2.11 Let $f(X)$ be a polynomial of degree n over $GF(2)$. The reciprocal of $f(X)$ is defined as

$$f^*(X) = X^n f\left(\frac{1}{X}\right).$$

a. Prove that $f^*(X)$ is irreducible over $GF(2)$ if and only if $f(X)$ is irreducible over $GF(2)$.

b. Prove that $f^*(X)$ is primitive if and only if $f(X)$ is primitive.

2.12 Find all the irreducible polynomials of degree 5 over $GF(2)$.

2.13 Construct a table for $GF(2^3)$ based on the primitive polynomial $p(X) = 1 + X + X^3$. Display the power, polynomial, and vector representations of each element. Determine the order of each element.

2.14 Construct a table for $GF(2^5)$ based on the primitive polynomial $p(X) = 1 + X^2 + X^5$. Let α be a primitive element of $GF(2^5)$. Find the minimal polynomials of α^3 and α^7.

2.15 Let β be an element in $GF(2^m)$. Let e be the smallest nonnegative integer such that $\beta^{2^e} = \beta$. Prove that $\beta^2, \beta^{2^2}, \cdots, \beta^{2^{e-1}}$, are all the distinct conjugates of β.

2.16 Prove Theorem 2.21.

2.17 Let α be a primitive element in $GF(2^4)$. Use Table 2.8 to find the roots of $f(X) = X^3 + \alpha^6 X^2 + \alpha^9 X + \alpha^9$.

2.18 Let α be a primitive element in $GF(2^4)$. Divide the polynomial $f(X) = \alpha^3 X^7 + \alpha X^6 + \alpha^7 X^4 + \alpha^2 X^2 + \alpha^{11} X + 1$ over $GF(2^4)$ by the polynomial $g(X) = X^4 + \alpha^3 X^2 + \alpha^5 X + 1$ over $GF(2^4)$. Find the quotient and the remainder (use Table 2.8).

2.19 Let α be a primitive element in $GF(2^4)$. Use Table 2.8 to solve the following simultaneous equations for X, Y, and Z:

$$\begin{aligned} X \quad + \alpha^5 Y + \quad Z \quad &= \alpha^7, \\ X \quad + \alpha Y \quad + \alpha^7 Z &= \alpha^9, \\ \alpha^2 X + \quad Y \quad + \alpha^6 Z &= \alpha. \end{aligned}$$

2.20 Let V be a vector space over a field F. For any element c in F, prove that $c \cdot \mathbf{0} = \mathbf{0}$.

2.21 Let V be a vector space over a field F. Prove that, for any c in F and any $\mathbf{v}$ in V, $(-c) \cdot \mathbf{v} = c \cdot (-\mathbf{v}) = -(c \cdot \mathbf{v})$.

2.22 Let S be a subset of the vector space V_n of all n-tuples over $GF(2)$. Prove that S is a subspace of V_n if for any $\mathbf{u}$ and $\mathbf{v}$ in S, $\mathbf{u} + \mathbf{v}$ is in S.

2.23 Prove that the set of polynomials over $GF(2)$ with degree $n - 1$ or less forms a vector space $GF(2)$ with dimension n.

2.24 Prove that $GF(2^m)$ is a vector space over $GF(2)$.

2.25 Construct the vector space V_5 of all 5-tuples over $GF(2)$. Find a three-dimensional subspace and determine its null space.

2.26 Given the matrices

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

show that the row space of $\mathbb{G}$ is the null space of $\mathbb{H}$, and vice versa.

2.27 Let S_1 and S_2 be two subspaces of a vector V. Show that the intersection of S_1 and S_2 is also a subspace in V.

2.28 Construct the vector space of all 3-tuples over $GF(3)$. Form a two-dimensional subspace and its dual space.

BIBLIOGRAPHY

1. G. Birkhoff and S. Maclane, *A Survey of Modern Algebra*, Macmillan, New York, 1953.

2. R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Ginn & Co., Boston, 1937.

3. A. Clark, *Elements of Abstract Algebra*, Dover, New York, 1984.

4. R. A. Dean, *Classical Abstract Algebra*, Harper & Row, New York, 1990.

5. T. W. Hungerford, *Abstract Algebra: An Introduction*, 2d ed., Saunders College Publishing, New York, 1997.

6. R. W. Marsh, *Table of Irreducible Polynomials over* GF*(2) through Degree 19*, NSA, Washington, D.C., 1957.

7. J. E. Maxfield and M. W. Maxfield, *Abstract Algebra and Solution by Radicals*, Dover, New York, 1992.

8. W. W. Peterson, *Error-Correcting Codes*, MIT Press, Cambridge, 1961.

9. B. L. Van der Waerden, *Modern Algebra*, Vols. 1 and 2, Ungar, New York, 1949.

Suppose $\mathbb{G}$ is in systematic form, $\mathbb{G} = [\mathbb{P}\ \mathbb{I}_{n/2}]$. From (3.47), we can easily see that

$$\mathbb{P} \cdot \mathbb{P}^T = \mathbb{I}_{n/2}. \tag{3.48}$$

Conversely, if a rate-$\frac{1}{2}$ $(n, n/2)$ linear block code C satisfies the condition of (3.47) [or (3.48)], then it is a self-dual code (the proof is left as a problem).

EXAMPLE 3.11

Consider the (8, 4) linear block code generated by the matrix

$$\mathbb{G} = \begin{bmatrix} 1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,0\,1\,1\,0\,0\,1\,1 \\ 0\,1\,0\,1\,0\,1\,0\,1 \end{bmatrix}.$$

The code has a rate $R = \frac{1}{2}$. It is easy to check that $\mathbb{G} \cdot \mathbb{G}^T = \mathbb{0}$. Therefore, it is a self-dual code.

There are many good self-dual codes but the most well known self-dual code is the (24, 12) Golay code, which will be discussed in Chapter 4.

PROBLEMS

3.1 Consider a systematic (8, 4) code whose parity-check equations are

$$\begin{aligned} v_0 &= u_1 + u_2 + u_3, \\ v_1 &= u_0 + u_1 + u_2, \\ v_2 &= u_0 + u_1 + u_3, \\ v_3 &= u_0 + u_2 + u_3. \end{aligned}$$

where u_0, u_1, u_2, and u_3, are message digits, and v_0, v_1, v_2, and v_3 are parity-check digits. Find the generator and parity-check matrices for this code. Show analytically that the minimum distance of this code is 4.

3.2 Construct an encoder for the code given in Problem 3.1.

3.3 Construct a syndrome circuit for the code given in Problem 3.1.

3.4 Let $\mathbb{H}$ be the parity-check matrix of an (n, k) linear code C that has both odd- and even-weight codewords. Construct a new linear code C_1 with the following parity-check matrix:

$$\mathbb{H}_1 = \left[\begin{array}{c|ccc} 0 & & & \\ 0 & & & \\ \vdots & & \mathbb{H} & \\ 0 & & & \\ \hline 1 & 1 & 1 \cdots & 1 \end{array}\right].$$

(Note that the last row of $\mathbb{H}_1$ consists of all 1's.)

a. Show that C_1 is an $(n + 1, k)$ linear code. C_1 is called an *extension* of C.

b. Show that every codeword of C_1 has even weight.

c. Show that C_1 can be obtained from C by adding an extra parity-check digit, denoted by v_∞, to the left of each codeword $\mathbf{v}$ as follows: (1) if $\mathbf{v}$ has odd weight, then $v_\infty = 1$, and (2) if $\mathbf{v}$ has even weight, then $v_\infty = 0$. The parity-check digit v_∞ is called an *overall parity-check* digit.

3.5 Let C be a linear code with both even- and odd-weight codewords. Show that the number of even-weight codewords is equal to the number of odd-weight codewords.

3.6 Consider an (n, k) linear code C whose generator matrix $\mathbf{G}$ contains no zero column. Arrange all the codewords of C as rows of a 2^k-by-n array.

a. Show that no column of the array contains only zeros.

b. Show that each column of the array consists of 2^{k-1} zeros and 2^{k-1} ones.

c. Show that the set of all codewords with zeros in a particular component position forms a subspace of C. What is the dimension of this subspace?

3.7 Prove that the Hamming distance satisfies the triangle inequality; that is, let $\mathbf{x}$, $\mathbf{y}$, and $\mathbf{z}$ be three n-tuples over $GF(2)$, and show that

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

3.8 Prove that a linear code is capable of correcting λ or fewer errors and simultaneously detecting $l (l > \lambda)$ or fewer errors if its minimum distance $d_{\min} \geq \lambda + l + 1$.

3.9 Determine the weight distribution of the (8, 4) linear code given in Problem 3.1. Let the transition probability of a BSC be $p = 10^{-2}$. Compute the probability of an undetected error of this code.

3.10 Because the (8, 4) linear code given in Problem 3.1 has minimum distance 4, it is capable of correcting all the single-error patterns and simultaneously detecting any combination of double errors. Construct a decoder for this code. The decoder must be capable of correcting any single error and detecting any double errors.

3.11 Let Γ be the ensemble of all the binary systematic (n, k) linear codes. Prove that a nonzero binary n-tuple $\mathbf{v}$ is contained in either exactly $2^{(k-1)(n-k)}$ codes in Γ or in none of the codes in Γ.

3.12 The (8, 4) linear code given in Problem 3.1 is capable of correcting 16 error patterns (the coset leaders of a standard array). Suppose that this code is used for a BSC. Devise a decoder for this code based on the table-lookup decoding scheme. The decoder is designed to correct the 16 most probable error patterns.

3.13 Let C_1 be an (n_1, k) linear systematic code with minimum distance d_1 and generator matrix $\mathbf{G}_1 = [\mathbf{P}_1 \ \mathbf{I}_k]$. Let C_2 be an (n_2, k) linear systematic code with minimum distance d_2 and generator matrix $\mathbf{G}_2 = [\mathbf{P}_2 \ \mathbf{I}_k]$. Consider an $(n_1 + n_2, k)$ linear code with the following parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} & & \mathbf{P}_1^T \\ \mathbf{I}_{n_1+n_2-k} & & \mathbf{I}_k \\ & & \mathbf{P}_2^T \end{bmatrix}.$$

Show that this code has a minimum distance of at least $d_1 + d_2$.

3.14 Show that the (8, 4) linear code C given in Problem 3.1 is self-dual.

3.15 For any binary (n, k) linear code with minimum distance (or minimum weight) $2t+1$ or greater, show that the number of parity-check digits satisfies the following inequality:

$$n - k \geq \log_2 \left[1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \right].$$

The preceding inequality gives an upper bound on the random-error-correcting capability t of an (n, k) linear code. This bound is known as the *Hamming*

bound [14]. (*Hint:* For an (n, k) linear code with minimum distance $2t + 1$ or greater, all the n-tuples of weight t or less can be used as coset leaders in a standard array.)

3.16 Show that the minimum distance $d_{\min}$ of an (n, k) linear code satisfies the following inequality:

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

(*Hint:* Use the result of Problem 3.6(b). This bound is known as the *Plotkin bound* [1-3].)

3.17 Show that there exists an (n, k) linear code with a minimum distance of at least d if

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

(*Hint:* Use the result of Problem 3.11 and the fact that the nonzero n-tuples of weight $d - 1$ or less can be at most in

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

(n, k) systematic linear codes.)

3.18 Show that there exists an (n, k) linear code with a minimum distance of at least $d_{\min}$ that satisfies the following inequality:

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

(*Hint:* See Problem 3.17. The second inequality provides a lower bound on the minimum distance attainable with an (n, k) linear code. This bound is known as the *Varsharmov–Gilbert* bound [1-3].)

3.19 Consider a rate-$\frac{1}{2}$ $(n, n/2)$ linear block code C with a generator matrix $\mathbb{G}$. Prove that C is self-dual if $\mathbb{G} \cdot \mathbb{G}^T = \mathbb{0}$.

3.20 Devise an encoder for the $(n, n-1)$ SPC code with only one memory element (or flip-flop) and one X-OR gate (or modulo-2 adder).

BIBLIOGRAPHY

1. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968; Rev. ed., Aegean Park Press, Laguna Hills, N.Y., 1984.

2. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2d ed., MIT Press, Cambridge, 1972.

3. F. J. MacWilliams and J. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

4. R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley, Reading, Mass., 1977.

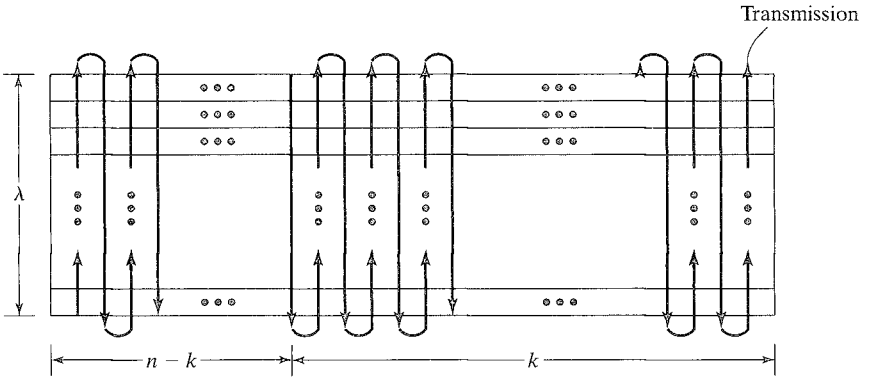


FIGURE 4.6: Transmission of an interleaved code.

is a correctable pattern for the original code C. The interleaving technique is very effective for deriving long, powerful codes for correcting errors that cluster to form *bursts*. This topic will be discussed in a later chapter.

Interleaving a single code can easily be generalized to interleaving several different codes of the same length. For $1 \leq i \leq \lambda$, let C_i be an (n, k_i) linear block code. Take λ codewords, one from each code, and arrange them as λ rows of a rectangular array as follows:

$$\begin{bmatrix} v_{1,0}, & v_{1,1}, & \cdots, & v_{1,n-1} \\ v_{2,0}, & v_{2,1}, & \cdots, & v_{2,n-1} \\ \vdots & & & \\ v_{\lambda,0}, & v_{\lambda,1}, & \cdots, & v_{\lambda,n-1} \end{bmatrix}. \tag{4.80}$$

Then, transmit this array column by column. This interleaving of λ codes results in an $(\lambda n, k_1 + k_2 + \cdots + k_\lambda)$ linear block code, denoted by $C^\lambda = C_1 * C_2 * \cdots * C_\lambda$. Each column of the array given in (4.80) is a binary λ-tuple. If each column of (4.80) is regarded as an element in Galois field $GF(2^\lambda)$, then C^λ may be regarded as a linear block code with symbols from $GF(2^\lambda)$.

The interleaving technique presented here is called *block interleaving*. Other types of interleaving will be discussed in later chapters and can be found in [26].

PROBLEMS

4.1 Form a parity-check matrix for the (15, 11) Hamming code. Devise a decoder for the code.

4.2 Show that Hamming codes achieve the Hamming bound (see Problem 3.15).

4.3 Show that the probability of an undetected error for Hamming codes of length $2^m - 1$ on a BSC with transition probability p satisfies the upper bound 2^{-m} for $p \leq 1/2$. (*Hint:* Use the inequality $(1 - 2p) \leq (1 - p)^2$.)

4.4 Compute the probability of an undetected error for the (15, 11) code on a BSC with transition probability $p = 10^{-2}$.

4.5 Devise a decoder for the (22, 16) SEC–DED code whose parity-check matrix is given in Figure 4.1(a).

4.6 Form the generator matrix of the first-order RM code RM(1, 3) of length 8. What is the minimum distance of the code? Determine its parity-check sums and devise a majority-logic decoder for the code. Decode the received vector $\mathbb{r} = (0\,1\,0\,0\,0\,1\,0\,1)$.

4.7 Form the generator matrix of the first-order RM code RM(1, 4) of length 16. What is the minimum distance of the code? Determine its parity-check sums and devise a majority-logic decoder for the code. Decode the received vector $\mathbb{r} = (0\,0\,1\,1\,0\,0\,1\,0\,0\,1\,1\,1\,0\,0\,1\,1)$.

4.8 Find the parity-check sums for the second-order RM code RM(2, 5) of length 32. What is the minimum distance of the code? Form the parity-check sums for the code. Describe the decoding steps.

4.9 Prove that the $(m - r - 1)$th-order RM code, RM$(m - r - 1, m)$, is the dual code of the rth-order RM code, RM(r, m).

4.10 Show that the RM(1, 3) and RM(2, 5) codes are self-dual.

4.11 Find a parity-check matrix for the RM(1, 4) code.

4.12 Construct the RM(2, 5) code of length 32 from RM codes of length 8 using $|\mathbb{u}|\mathbb{u} + \mathbb{v}|$-construction.

4.13 Using the $|\mathbb{u}|\mathbb{u} + \mathbb{v}|$-construction, decompose the RM(2, 5) code into component codes that are either repetition codes of dimension 1 or even parity-check codes of minimum distance 2.

4.14 Determine the Boolean polynomials that give the codewords of the RM(1, 3) code.

4.15 Use Boolean representation to show that the RM(r, m) code can be constructed from RM$(r, m - 1)$ and RM$(r - 1, m - 1)$ codes.

4.16 Construct the RM(2, 4) code from the RM(2, 3) and RM(1, 3) codes using one-level squaring construction. Find its generator matrix in the form of (4.53) or (4.68).

4.17 Using two-level squaring construction, express the generator matrix of the RM(2, 4) code in the forms of (4.60) and (4.61).

4.18 Prove that the (24, 12) Golay code is self-dual. (*Hint:* Show that $\mathbb{G} \cdot \mathbb{G}^T = 0$.)

4.19 Design an encoding circuit for the (24, 12) Golay code.

4.20 Suppose that the (24, 12) Golay code is used for error correction. Decode the following received sequences:

a. $\mathbb{r} = (1\,0\,1\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0\,0\,1\,1)$,

b. $\mathbb{r} = (0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1)$.

4.21 Show that the digits for checking the parity-check digits of a product code array shown in Figure 4.3 are the same no matter whether they are formed by using the parity-check rules for C_2 on columns or the parity-check rules for C_1 on rows.

4.22 Prove that the minimum distance of the incomplete product of an (n_1, k_1, d_1) linear code and an (n_2, k_2, d_2) linear code is $d_1 + d_2 - 1$.

4.23 The incomplete product of the $(n_1, n_1 - 1, 2)$ and the $(n_2, n_2 - 1, 2)$ even parity-check codes has a minimum distance of 3. Devise a decoding algorithm for correcting a single error in the information part of a code array.

For $0 \leq l < n_0$, let $\mathbb{Q}_l$ be the $mk_0 \times m$ submatrix that is formed by taking the lth columns from $\mathbb{M}_0, \mathbb{M}_1, \cdots, \mathbb{M}_{m-1}$. Then, we can put $\mathbb{G}$ in the following form:

$$\mathbb{G}_c = [\mathbb{Q}_0, \mathbb{Q}_1, \cdots, \mathbb{Q}_{n_0-1}].$$

Each column of $\mathbb{Q}_l$ consists of mk_0 bits that are regarded as m k_0-bit bytes (a *byte* is a group of k_0 binary digits). In terms of bytes, $\mathbb{Q}_l$ is regarded as an $m \times m$ matrix that has the following cyclic structure: (1) each row is the cyclic shift (to the right) of the row immediately above it, and the top row is the cyclic shift of the bottom row; (2) each column is the downward cyclic shift of the column on its left, and the leftmost column is the downward cyclic shift of the rightmost column. The matrix $\mathbb{Q}_l$ is called a *circulant*. Therefore, $\mathbb{G}_c$ consists of n_0 circulants. Most often, quasi-cyclic codes are studied in circulant form.

EXAMPLE 5.14

Consider the (15, 5) quasi-cyclic code with parameters $m = 5$, $n_0 = 3$, and $k_0 = 1$ that is generated by the following generator matrix:

$$\mathbb{G} = \begin{bmatrix} 001 & 100 & 010 & 110 & 110 \\ 110 & 001 & 100 & 010 & 110 \\ 110 & 110 & 001 & 100 & 010 \\ 010 & 110 & 110 & 001 & 100 \\ 100 & 010 & 110 & 110 & 001 \end{bmatrix}.$$
$$\mathbb{M}_0 \quad \mathbb{M}_1 \quad \mathbb{M}_2 \quad \mathbb{M}_3 \quad \mathbb{M}_4$$

This quasi-cyclic code has a minimum distance of 7. In circulant form, the generator matrix takes the following form:

$$\mathbb{G} = \begin{bmatrix} 01011 & 00111 & 10000 \\ 10101 & 10011 & 01000 \\ 11010 & 11001 & 00100 \\ 01101 & 11100 & 00010 \\ 10110 & 01110 & 00001 \end{bmatrix}.$$
$$\mathbb{Q}_0 \quad \mathbb{Q}_1 \quad \mathbb{Q}_2$$

PROBLEMS

5.1 Consider the (15, 11) cyclic Hamming code generated by $\mathbf{g}(X) = 1 + X + X^4$.
- **a.** Determine the parity polynomial $\mathbf{h}(X)$ of this code.
- **b.** Determine the generator polynomial of its dual code.
- **c.** Find the generator and parity matrices in systematic form for this code.

5.2 Devise an encoder and a decoder for the (15, 11) cyclic Hamming code generated by $\mathbf{g}(X) = 1 + X + X^4$.

5.3 Show that $\mathfrak{g}(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$ generates a (21, 11) cyclic code. Devise a syndrome computation circuit for this code. Let $\mathfrak{r}(X) = 1 + X^5 + X^{17}$ be a received polynomial. Compute the syndrome of $\mathfrak{r}(X)$. Display the contents of the syndrome register after each digit of $\mathfrak{r}$ has been shifted into the syndrome computation circuit.

5.4 Shorten this (15, 11) cyclic Hamming by deleting the seven leading high-order message digits. The resultant code is an (8, 4) shortened cyclic code. Design a decoder for this code that eliminates the extra shifts of the syndrome register.

5.5 Shorten the (31, 26) cyclic Hamming code by deleting the 11 leading high-order message digits. The resultant code is a (20, 15) shortened cyclic code. Devise a decoding circuit for this code that requires no extra shifts of the syndrome register.

5.6 Let $\mathfrak{g}(X)$ be the generator polynomial of a binary cyclic code of length n.

a. Show that if $\mathfrak{g}(X)$ has $X + 1$ as a factor, the code contains no codewords of odd weight.

b. If n is odd and $X + 1$ is not a factor of $\mathfrak{g}(X)$, show that the code contains a codeword consisting of all 1's.

c. Show that the code has a minimum weight of at least 3 if n is the smallest integer such that $\mathfrak{g}(X)$ divides $X^n + 1$.

5.7 Consider a binary (n, k) cyclic code C generated by $\mathfrak{g}(X)$. Let

$$\mathfrak{g}^*(X) = X^{n-k}\mathfrak{g}(X^{-1})$$

be the reciprocal polynomial of $\mathfrak{g}(X)$.

a. Show that $\mathfrak{g}^*(X)$ also generates an (n, k) cyclic code.

b. Let C^* denote the cyclic code generated by $\mathfrak{g}^*(X)$. Show that C and C^* have the same weight distribution.

(*Hint:* Show that

$$\mathfrak{v}(X) = v_0 + v_1X + \cdots + v_{n-2}X^{n-2} + v_{n-1}X^{n-1}$$

is a code polynomial in C if and only if

$$X^{n-1}\mathfrak{v}(X^{-1}) = v_{n-1} + v_{n-2}X + \cdots + v_1X^{n-2} + v_0X^{n-1}$$

is a code polynomial in C^*.)

5.8 Consider a cyclic code C of length n that consists of both odd-weight and even-weight codewords. Let $\mathfrak{g}(X)$ and $A(z)$ be the generator polynomial and weight enumerator for this code. Show that the cyclic code generated by $(X + 1)\mathfrak{g}(X)$ has weight enumerator

$$A_1(z) = \tfrac{1}{2}[A(z) + A(-z)].$$

5.9 Suppose that the (15, 10) cyclic Hamming code of minimum distance 4 is used for error detection over a BSC with transition probability $p = 10^{-2}$. Compute the probability of an undetected error, $P_u(E)$, for this code.

5.10 Consider the $(2^m - 1, 2^m - m - 2)$ cyclic Hamming code C generated by $\mathfrak{g}(X) = (X + 1)\mathfrak{p}(X)$, where $\mathfrak{p}(X)$ is a primitive polynomial of degree m. An error pattern of the form

$$\mathfrak{e}(X) = X^i + X^{i+1}$$

is called a *double-adjacent-error pattern*. Show that no two double-adjacent-error patterns can be in the same coset of a standard array for C. Therefore, the code is capable of correcting all the single-error patterns and all the double-adjacent-error patterns.

5.11 Devise a decoding circuit for the (7, 3) Hamming code generated by $\mathbf{g}(X) = (X+1)(X^3+X+1)$. The decoding circuit corrects all the single-error patterns and all the double-adjacent-error patterns (see Problem 5.10).

5.12 For a cyclic code, if an error pattern $\mathbf{e}(X)$ is detectable, show that its ith cyclic shift $e^{(i)}(X)$ is also detectable.

5.13 In the decoding of an (n, k) cyclic code, suppose that the received polynomial $\mathbf{r}(X)$ is shifted into the syndrome register from the right end, as shown in Figure 5.11. Show that when a received digit r_i is detected in error and is corrected, the effect of error digit e_i on the syndrome can be removed by feeding e_i into the syndrome register from the right end, as shown in Figure 5.11.

5.14 Let $\mathbf{v}(X)$ be a code polynomial in a cyclic code of length n. Let l be the smallest integer such that

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

Show that if $l \neq 0$, l is a factor of n.

5.15 Let $\mathbf{g}(X)$ be the generator polynomial of an (n, k) cyclic code C. Suppose C is interleaved to a depth of λ. Prove that the interleaved code C^{λ} is also cyclic and its generator polynomial is $\mathbf{g}(X^{\lambda})$.

5.16 Construct all the binary cyclic codes of length 15. (*Hint:* Using the fact that $X^{15}+1$ has all the nonzero elements of $GF(2^4)$ as roots and using Table 2.9, factor $X^{15}+1$ as a product of irreducible polynomials.)

5.17 Let β be a nonzero element in the Galois field $GF(2^m)$, and $\beta \neq 1$. Let $\boldsymbol{\phi}(X)$ be the minimum polynomial of β. Is there a cyclic code with $\boldsymbol{\phi}(X)$ as the generator polynomial? If your answer is yes, find the shortest cyclic code with $\boldsymbol{\phi}(X)$ as the generator polynomial.

5.18 Let β_1 and β_2 be two distinct nonzero elements in $GF(2^m)$. Let $\boldsymbol{\phi}_1(X)$ and $\boldsymbol{\phi}_2(X)$ be the minimal polynomials of β_1 and β_2, respectively. Is there a cyclic code with $\mathbf{g}(X) = \boldsymbol{\phi}_1(X) \cdot \boldsymbol{\phi}_2(X)$ as the generator polynomial? If your answer is yes, find the shortest cyclic code with $\mathbf{g}(X) = \boldsymbol{\phi}_1(X) \cdot \boldsymbol{\phi}_2(X)$ as the generator polynomial.

5.19 Consider the Galois field $GF(2^m)$, which is constructed based on the primitive polynomial $\mathbf{p}(X)$ of degree m. Let α be a primitive element of $GF(2^m)$ whose minimal polynomial is $\mathbf{p}(X)$. Show that every code polynomial in the Hamming code generated by $\mathbf{p}(X)$ has α and its conjugates as roots. Show that any binary polynomial of degree $2^m - 2$ or less that has α as a root is a code polynomial in the Hamming code generated by $\mathbf{p}(X)$.

5.20 Let C_1 and C_2 be two cyclic codes of length n that are generated by $\mathbf{g}_1(X)$ and $\mathbf{g}_2(X)$, respectively. Show that the code polynomials common to both C_1 and C_2 also form a cyclic code C_3. Determine the generator polynomial of C_3. If d_1 and d_2 are the minimum distances of C_1 and C_2, respectively, what can you say about the minimum distance of C_3?

5.21 Show that the probability of an undetected error for the distance-4 cyclic Hamming codes is upper bounded by $2^{-(m+1)}$.

5.22 Let C be a $(2^m-1, 2^m-m-1)$ Hamming code generated by a primitive polynomial $\mathbf{p}(X)$ of degree m. Let C_d be the dual code of C. Then, C_d is a $(2^m-1, m)$ cyclic code generated by

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

where

$$\mathbb{h}(X) = \frac{X^{2^m-1}+1}{\mathbb{p}(X)}.$$

a. Let $\mathbb{v}(X)$ be a codeword in C_d and let $\mathbb{v}^{(i)}(X)$ be the ith cyclic shift of $\mathbb{v}(X)$. Show that for $1 \leq i \leq 2^m - 2$, $\mathbb{v}^{(i)}(X) \neq \mathbb{v}(X)$.

b. Show that C_d contains the all-zero codeword and $2^m - 1$ codewords of weight 2^{m-1}.

(*Hint:* For part (a), use (5.1) and the fact that the smallest integer n such that $X^n + 1$ is divisible by $\mathbb{p}(X)$ is $2^m - 1$. For part (b), use the result of Problem 3.6(b).)

5.23 For an (n, k) cyclic code, show that the syndrome of an end-around burst of length $n - k$ cannot be zero.

5.24 Design a Meggitt decoder that decodes a received polynomial $\mathbb{r}(X) = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1}$ from the lowest-order received digit r_0 to the highest-order received digit r_{n-1}. Describe the decoding operation and the syndrome modification after each correction.

5.25 Consider the (15, 5) cyclic code generated by the following polynomial:

$$\mathbb{g}(X) = 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}.$$

This code has been proved to be capable of correcting any combination of three or fewer errors. Suppose that this code is to be decoded by the simple error-trapping decoding scheme.

a. Show that all the double errors can be trapped.

b. Can all the error patterns of three errors be trapped? If not, how many error patterns of three errors cannot be trapped?

c. Devise a simple error-trapping decoder for this code.

5.26 a. Devise a simple error-trapping decoder for the (23, 12) Golay code.

b. How many error patterns of double errors cannot be trapped?

c. How many error patterns of three errors cannot be trapped?

5.27 Suppose that the (23, 12) Golay code is used only for error correction on a BSC with transition probability p. If Kasami's decoder of Figure 5.18 is used for decoding this code, what is the probability of a decoding error? (*Hint:* Use the fact that the (23, 12) Golay code is a perfect code.)

5.28 Use the decoder of Figure 5.18 to decode the following received polynomials:

a. $\mathbb{r}(X) = X^5 + X^{19}$

b. $\mathbb{r}(X) = X^4 + X^{11} + X^{21}$

At each step in the decoding process, write down the contents of the syndrome register.

5.29 Consider the following binary polynomial:

$$\mathbb{g}(X) = (X^3 + 1)\mathbb{p}(X),$$

where (X^3+1) and $\mathbb{p}(X)$ are relatively prime, and $\mathbb{p}(X)$ is an irreducible polynomial of degree m with $m \geq 3$. Let n be the smallest integer such that $\mathbb{g}(X)$ divides $X^n + 1$. Thus, $\mathbb{g}(X)$ generates a cyclic code of length n.

a. Show that this code is capable of correcting all the single-error, double-adjacent-error, and triple-adjacent-error patterns. (*Hint:* Show that these error patterns can be used as coset leaders of a standard array for the code.)

b. Devise an error-trapping decoder for this code. The decoder must be capable of correcting all the single-error, double-adjacent-error, and triple-adjacent-error patterns. Design a combinational logic circuit whose output is 1 when the errors are trapped in the appropriate stages of the syndrome register.

c. Suppose that $\mathbf{p}(X) = 1 + X + X^4$, which is a primitive polynomial of degree 4. Determine the smallest integer n such that $\mathbf{g}(X) = (X^3 + 1)\mathbf{p}(X)$ divides $X^n + 1$.

5.30 Let C_1 be the (3, 1) cyclic code generated by $\mathbf{g}_1(X) = 1 + X + X^2$, and let C_2 be the (7, 3) maximum-length code generated by $\mathbf{g}_2(X) = 1 + X + X^2 + X^4$. Find the generator and parity polynomials of the cyclic product of C_1 and C_2. What is the minimum distance of this product code? Discuss its error-correcting capability.

5.31 Devise an encoding circuit for the (15, 5) quasi-cyclic code given in Example 5.14.

BIBLIOGRAPHY

1. E. Prange, "Cyclic Error-Correcting Codes in Two Symbols," *AFCRC-TN-57, 103*, Air Force Cambridge Research Center, Cambridge, Mass., September 1957.

2. E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968. (Rev. ed., Aegean Park Press, Laguna Hills, Calif., 1984.)

3. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2d ed., MIT Press, Cambridge, Mass., 1972.

4. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

5. R. E. Blahut, *Theory and Practice of Error Control Codes,* Addison-Wesley, Reading, Mass., 1984.

6. R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley, Reading, Mass., 1977.

7. G. Clark and J. Cain, *Error-Correction Codes for Digital Communications,* Plenum, New York, 1981.

8. S. A. Vanstone and P. C. van Oorschot, *An Introduction to Error Correcting Codes with Applications*, Kluwer Academic, Boston, Mass., 1989.

9. S. B. Wicker, *Error Control Systems for Digital Communication and Storage,* Prentice Hall, Englewood Cliffs, N.J., 1995.

10. W. W. Peterson, "Encoding and Error-Correction Procedures for the Bose–Chaudhuri Codes," *IRE Trans. Inform. Theory*, IT-6, 459–70, September 1960.

11. J. E. Meggitt, "Error Correcting Codes and Their Implementation," *IRE Trans. Inform. Theory*, IT-7: 232–44, October 1961.

summarize the preceding results above as follows: For a t-error-correcting primitive BCH code of length $n = 2^m - 1$ with number of parity-check digits $n - k = mt$ and $m \geq m_0(t)$, its probability of an undetected error on a BSC with transition probability p satisfies the following bounds:

$$P_u(E) \leq \begin{cases} (1 + \lambda_0 \cdot n^{-1/10})2^{-n[1-R+E(\varepsilon,p)]} & \text{for } p < \varepsilon \\ (1 + \lambda_0 \cdot n^{-1/10})2^{-n(1-R)} & \text{for } p \geq \varepsilon \end{cases} \tag{6.52}$$

where $\varepsilon = (2t + 1)/n$, $R = k/n$, and λ_0 is a constant.

The foregoing analysis indicates that primitive BCH codes are very effective for error detection on a BSC.

6.10 REMARKS

BCH codes form a subclass of a very special class of linear codes known as *Goppa codes* [21, 22]. It has been proved that the class of Goppa codes contains good codes. Goppa codes are in general noncyclic (except the BCH codes), and they can be decoded much like BCH codes. The decoding also consists of four steps: (1) compute the syndromes; (2) determine the error-location polynomial $\sigma(X)$; (3) find the error-location numbers; and (4) evaluate the error values (this step is not needed for binary Goppa codes). Berlekamp's iterative algorithm for finding the error-location polynomial for a BCH code can be modified for finding the error-location polynomial for Goppa codes [26]. Discussion of Goppa codes is beyond the scope of this introductory book. Moreover, implementation of BCH codes is simpler than that of Goppa codes, and no Goppa codes better than BCH codes have been found. For details on Goppa codes, the reader is referred to [26]–[30].

Our presentation of BCH codes and their implementation is given in the time domain. BCH codes also can be defined and implemented in the frequency domain using Fourier transforms over Galois fields. Decoding BCH codes in the frequency domain sometimes offers computational or implementation advantages. This topic will be discussed in Chapter 7.

PROBLEMS

6.1 Consider the Galois field $GF(2^4)$ given by Table 2.8. The element $\beta = \alpha^7$ is also a primitive element. Let $\mathbf{g}_0(X)$ be the lowest-degree polynomial over $GF(2)$ that has

$$\beta, \beta^2, \beta^3, \beta^4$$

as its roots. This polynomial also generates a double-error-correcting primitive BCH code of length 15.

a. Determine $\mathbf{g}_0(X)$.

b. Find the parity-check matrix for this code.

c. Show that $\mathbf{g}_0(X)$ is the reciprocal polynomial of the polynomial $\mathbf{g}(X)$ that generates the (15, 7) double-error-correcting BCH code given in Example 6.1.

6.2 Determine the generator polynomials of all the primitive BCH codes of length 31. Use the Galois field $GF(2^5)$ generated by $\mathbf{p}(X) = 1 + X^2 + X^5$.

6.3 Suppose that the double-error-correcting BCH code of length 31 constructed in Problem 6.2 is used for error correction on a BSC. Decode the received polynomials $\mathbb{r}_1(X) = X^7 + X^{30}$ and $\mathbb{r}_2(X) = 1 + X^{17} + X^{28}$.

6.4 Consider a t-error-correcting primitive binary BCH code of length $n = 2^m - 1$. If $2t + 1$ is a factor of n, prove that the minimum distance of the code is exactly $2t + 1$. (*Hint*: Let $n = l(2t + 1)$. Show that $(X^n + 1)/(X^l + 1)$ is a code polynomial of weight $2t + 1$.)

6.5 Is there a binary t-error-correcting BCH code of length $2^m + 1$ for $m \geq 3$ and $t < 2^{m-1}$? If there is such a code, determine its generator polynomial.

6.6 Consider the field $GF(2^4)$ generated by $\mathbb{p}(X) = 1 + X + X^4$ (see Table 2.8). Let α be a primitive element in $GF(2^4)$ such that $\mathbb{p}(\alpha) = 0$. Devise a circuit that is capable of multiplying any element in $GF(2^4)$ by α^7.

6.7 Devise a circuit that is capable of multiplying any two elements in $GF(2^5)$. Use $\mathbb{p}(X) = 1 + X^2 + X^5$ to generate $GF(2^5)$.

6.8 Devise a syndrome computation circuit for the binary double-error-correcting (31, 21) BCH code.

6.9 Devise a Chien's searching circuit for the binary double-error-correcting (31, 21) BCH code.

6.10 Consider the Galois field $GF(2^6)$ given by Table 6.2. Let $\beta = \alpha^3, l_0 = 2$, and $d = 5$. Determine the generator polynomial of the BCH code that has

$$\beta^2, \beta^3, \beta^4, \beta^5$$

as its roots (the general form presented at the end of Section 6.1). What is the length of this code?

6.11 Let $l_0 = -t$ and $d = 2t + 2$. Then we obtain a BCH code of designed distance $2t + 2$ whose generator polynomial has

$$\beta^{-t}, \cdots, \beta^{-1}, \beta^0, \beta^1, \cdots, \beta^t$$

and their conjugates as all its roots.

𝕒. Show that this code is a reversible cyclic code.

𝕓. Show that if t is odd, the minimum distance of this code is at least $2t + 4$. (*Hint:* Show that $\beta^{-(t+1)}$ and β^{t+1} are also roots of the generator polynomial.)

BIBLIOGRAPHY

1. A. Hocquenghem, "Codes corecteurs d'erreurs," *Chiffres*, 2: 147–56, 1959.

2. R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes," *Inform. Control*, 3: 68–79, March 1960.

3. W. W. Peterson, "Encoding and Error-Correction Procedures for the Bose–Chaudhuri Codes," *IRE Trans. Inform. Theory*, IT-6: 459–70, September 1960.

4. D. Gorenstein and N. Zierler, "A Class of Cyclic Linear Error-Correcting Codes in p^m Symbols," *J. Soc. Ind. Appl. Math.*, 9: 107–214, June 1961.

5. I. S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Fields," *J. Soc. Ind. Appl. Math.*, 8: 300–304, June 1960.

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

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

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

Then, the estimated error polynomial is

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

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

PROBLEMS

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

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

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

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

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

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

using the Berlekamp algorithm.

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

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

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

using the Euclidean algorithm.

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

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

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

with the Euclidean algorithm.

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

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

7.11 Let α be a primitive element in $GF(2^m)$. Consider the $(2^m - 1, k)$ RS code of length of $2^m - 1$ and minimum distance d generated by

$$\mathbf{g}(X) = (X - \alpha)(X - \alpha^2)...(X - \alpha^{d-1}).$$

Prove that extending each codeword $v = (v_0, v_1, \cdots, v_{2^m-2})$ by adding an overall parity-check symbol

$$v_\infty = -\sum_{i=0}^{2^m-2} v_i$$

produces a $(2^m, k)$ code with a minimum distance of $d + 1$.

7.12 Consider a t-symbol error-correcting RS code over $GF(2^m)$ with the following parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix},$$

where $n = 2^m - 1$, and α is a primitive element in $GF(2^m)$. Consider the extended Reed–Solomon code with the following parity-check matrix:

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 1 & \\ 0 & 0 & \\ \vdots & \vdots & \mathbf{H} \\ 0 & 0 & \\ 1 & 0 & \end{bmatrix}$$

Prove that the extended code also has a minimum distance of $2t + 1$.

7.13 Let $\mathbf{a}(X) = a_0 + a_1X + \cdots + a_{k-1}X^{k-1}$ be a polynomial of degree $k - 1$ or less over $GF(2^m)$. There are $(2^m)^k$ such polynomials. Let α be a primitive element in $GF(2^m)$. For each polynomial $\mathbf{a}(X)$, form the following polynomial of degree $2^m - 2$ or less over $GF(2^m)$:

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

Prove that the set $\{\mathbf{v}(X)\}$ forms the $(2^m - 1, k)$ RS code over $GF(2^m)$. (*Hint:* Show that $\mathbf{v}(X)$ has $\alpha, \alpha^2, \cdots, \alpha^{2^m-k-1}$ as roots). This original definition of a RS code is given by Reed and Solomon [1].

BIBLIOGRAPHY

1. I. S. Reed and G. Solomon, "Polynomial Codes over Certain Fields," *J. Soc. Ind. Appl. Math.*, 8: 300–304, June 1960.

2. D. Gorenstein and N. Zierler, "A Class of Cyclic Linear Error-Correcting Codes in p^m Symbols," *J. Soc. Ind. Appl. Math.*, 9: 107–214, June 1961.

3. R. T. Chien, "Cyclic Decoding Procedure for the Bose–Chaudhuri–Hocquenghem Codes," *IEEE Trans. Inf. Theory*, IT-10: 357–63, October 1964.

exactly the same way, simply by replacing 2 with p and $GF(2^s)$ with $GF(p^s)$. Construction of codes based on the flats and points in these finite geometries results in a much larger class of majority-logic decodable codes. Construction of finite geometries over $GF(p^s)$ and their application to the construction of low-density parity-check codes will be discussed in Chapter 17.

PROBLEMS

8.1 Consider the (31, 5) maximum-length code whose parity-check polynomial is $\mathbf{p}(X) = 1 + X^2 + X^5$. Find all the polynomials orthogonal on the digit position X^{30}. Devise both type-I and type-II majority-logic decoders for this code.

8.2 $P = \{0, 2, 3\}$ is a perfect simple difference set. Construct a difference-set code based on this set.

a. What is the length n of this code?

b. Determine its generator polynomial.

c. Find all the polynomials orthogonal on the highest-order digit position X^{n-1}.

d. Construct a type-I majority-logic decoder for this code.

8.3 Example 8.1 shows that the (15, 7) BCH code is one-step majority-logic decodable and is capable of correcting any combination of two or fewer errors. Show that the code is also capable of correcting some error patterns of three errors and some error patterns of four errors. List some of these error patterns.

8.4 Consider an (11, 6) linear code whose parity-check matrix is

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

(This code is not cyclic.)

a. Show that the minimum distance of this code is exactly 4.

b. Let $\mathbf{e} = (e_0, e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10})$ be an error vector. Find the syndrome bits in terms of error digits.

c. Construct all possible parity-check sums orthogonal on each message error digit e_i for $i = 5, 6, 7, 8, 9, 10$.

d. Is this code completely orthogonalizable in one step?

8.5 Let $m = 6$. Express the integer 43 in radix-2 form. Find all the nonzero proper descendants of 43.

8.6 Let α be a primitive element of $GF(2^4)$ given by Table 2.8. Apply the affine permutation $Z = \alpha^3 Y + \alpha^{11}$ to the following vector of 16 components:

	Location Numbers															
	α^∞	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
$\mathbf{u} =$	(1	1	1	0	0	1	0	1	0	1	1	0	0	0	0	1)

What is the resultant vector?

8.7 Let $m = 6$. Then, $2^6 - 1$ can be factored as follows: $2^6 - 1 = 7 \times 9$. Let $J = 9$ and $L = 7$. Find the generator polynomial of the type-I DTI code of length 63 and $J = 9$ (use Table 6.2). Find all the polynomials (or vectors) orthogonal on the digit position X^{62} (or α^{62}).

8.8 Find the generator polynomial of the type-I DTI code of length 63 and $J = 7$. Find all the polynomials orthogonal on the digit position X^{62}.

8.9 Show that the all-one vector is not a code vector in a maximum-length code.

8.10 Let $\mathbb{v}(X) = v_0 + v_1 X + \cdots + v_{2^m-2} X^{2^m-2}$ be a nonzero code polynomial in the $(2^m - 1, m)$ maximum-length code whose parity-check polynomial is $\mathbb{p}(X)$. Show that the other $2^m - 2$ nonzero code polynomials are cyclic shifts of $\mathbb{v}(X)$. (*Hint:* Let $\mathbb{v}^{(i)}(X)$ and $\mathbb{v}^{(j)}(X)$ be the ith and jth cyclic shifts of $\mathbb{v}(X)$, respectively, with $0 \le i < j < 2^m - 2$. Show that $\mathbb{v}^{(i)}(X) \neq \mathbb{v}^{(j)}(X)$.)

8.11 Arrange the 2^m code vectors of a maximum-length code as rows of a $2^m \times (2^m - 1)$ array.

- a. Show that each column of this array has 2^{m-1} ones and 2^{m-1} zeros.
- b. Show that the weight of each nonzero code vector is exactly 2^{m-1}.

8.12 Example 8.12 shows that the (15, 5) BCH code is two-step majority-logic decodable and is capable of correcting any combination of three or fewer errors. Devise a type-I majority-logic decoder for this code.

8.13 Show that the extended cyclic Hamming code is invariant under the affine permutations.

8.14 Show that the extended primitive BCH code is invariant under the affine permutations.

8.15 Let $P = \{l_0, l_1, l_2, \ldots, l_{2^s}\}$ be a perfect simple difference set of order 2^s such that

$$0 \le l_0 < l_1 < l_2 < \cdots < l_{2^s} \le 2^s(2^s + 1).$$

Construct a vector of $n = 2^{2s} + 2^s + 1$ components,

$$\mathbb{v} = (v_0, v_1, \ldots, v_{n-1}),$$

whose nonzero components are $v_{l_0}, v_{l_1}, \ldots, v_{l_{2^s}}$; that is,

$$v_{l_0} = v_{l_1} = \cdots = v_{l_{2^s}} = 1.$$

Consider the following $n \times 2n$ matrix:

$$\mathbb{G} = [\mathbb{Q}\ \mathbb{I}_n],$$

where (1) $\mathbb{I}_n$ is an $n \times n$ identity matrix, and (2) $\mathbb{Q}$ is an $n \times n$ matrix whose n rows are $\mathbb{v}$ and $n - 1$ cyclic shifts of $\mathbb{v}$. The code generated by $\mathbb{G}$ is a $(2n, n)$ linear (not cyclic) code whose parity-check matrix is

$$\mathbb{H} = [\mathbb{I}_n\ \mathbb{Q}^T].$$

- a. Show that $J = 2^s + 1$ parity-check sums orthogonal on any message error digit can be formed.
- b. Show that the minimum distance of this code is $d = J + 1 = 2^s + 2$. (This code is a half-rate *quasi-cyclic code* [20].)

8.16 Prove that if J parity-check sums orthogonal on any digit position can be formed for a linear code (cyclic or noncyclic), the minimum distance of the code is at least $J + 1$.

8.17 Consider the Galois field $GF(2^4)$ given by Table 2.8. Let $\beta = \alpha^5$. Then, $\{0, 1, \beta, \beta^2\}$ form the subfield $GF(2^2)$ of $GF(2^4)$. Regard $GF(2^4)$ as the two-dimensional Euclidean geometry over $GF(2^2)$, $\mathrm{EG}(2, 2^2)$. Find all the 1-flats that pass through the point α^7.

8.18 Consider the Galois field $GF(2^6)$ given by Table 6.2. Let $\beta = \alpha^{21}$. Then, $\{0, 1, \beta, \beta^2\}$ form the subfield $GF(2^2)$ of $GF(2^6)$. Regard $GF(2^6)$ as the three-dimensional Euclidean geometry EG$(3, 2^2)$.

a. Find all the 1-flats that pass through the point α^{63}.

b. Find all the 2-flats that intersect on the 1-flat, $\{\alpha^{63} + \eta\alpha\}$, where $\eta \in GF(2^2)$.

8.19 Regard $GF(2^6)$ as the two-dimensional Euclidean geometry EG$(2, 2^3)$. Let $\beta = \alpha^9$. Then, $\{0, 1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6\}$ form the subfield $GF(2^3)$ of $GF(2^6)$. Determine all the 1-flats that pass through the point α^{21}.

8.20 Let $m = 2$ and $s = 3$.

a. Determine the 2^3-weight of 47.

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

c. Determine all the positive integers h less than 63 such that

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

8.21 Find the generator polynomial of the first-order cyclic RM code of length $2^5 - 1$. Describe how to decode this code.

8.22 Find the generator polynomial of the third-order cyclic RM code of length $2^6 - 1$. Describe how to decode this code.

8.23 Let $m = 2$ and $s = 3$. Find the generator polynomial of the $(0, 3)$th-order EG code of length $2^{2\times 3} - 1$. This code is one-step majority-logic decodable. Find all the polynomials orthogonal on the digit location α^{62} where α is a primitive element in $GF(2^{2\times 3})$. Design a type-I majority-logic decoder for this code.

8.24 Let $m = 3$ and $s = 2$. Find the generator polynomial of the $(1, 2)$th-order twofold EG code of length $2^{3\times 2} - 1$. Describe how to decode this code.

8.25 Prove that the $(m-2)$th-order cyclic RM code of length $2^m - 1$ is a Hamming code. (*Hint:* Show that its generator polynomial is a primitive polynomial of degree m.)

8.26 Prove that the even-weight codewords of the first-order cyclic RM code of length $2^m - 1$ form the maximum-length code of length $2^m - 1$.

8.27 Let $0 < \mu < m - 1$. Prove that the even-weight codewords of the $(m - \mu - 1)$th-order cyclic RM code of length $2^m - 1$ form the dual of the μth-order RM code of length $2^m - 1$. (*Hint:* Let $\mathbf{g}(X)$ be the generator polynomial of the $(m - \mu - 1)$th-order cyclic RM code C. Show that the set of even-weight codewords of C is a cyclic code generated by $(X + 1)\mathbf{g}(X)$. Show that the dual of the μth-order cyclic RM code is also generated by $(X + 1)\mathbf{g}(X)$.)

8.28 The μth-order cyclic RM code of length $2^m - 1$ has a minimum distance of $d_{\min} = 2^{m-\mu} - 1$. Prove that this RM code is a subcode of the primitive BCH code of length $2^m - 1$ and designed distance $2^{m-\mu} - 1$. (*Hint:* Let $\mathbf{g}(X)_{RM}$ be the generator polynomial of the RM code and let $\mathbf{g}(X)_{BCH}$ be the generator polynomial of the BCH code. Prove that $\mathbf{g}(X)_{BCH}$ is a factor of $\mathbf{g}(X)_{RM}$.)

8.29 Show that extended RM codes are invariant under the affine permutations.

8.30 Let $m = 3$, $s = 2$ and $\mu = 2$. Find the generator polynomial of the $(2, 2)$th-order PG code constructed based on the projective geometry PG$(3, 2^2)$. This code is two-step majority-logic decodable. Find all the orthogonal polynomials at each step of orthogonalization.

8.31 Let $\mathcal{L}$ be a line in the two-dimensional Euclidean geometry EG$(2, 2^s)$ that does not pass through the origin. Let $\mathbf{v}_{\mathcal{L}}$ be the incidence vector of $\mathcal{L}$. For $0 < i \le 2^{2s} - 2$, let $\mathbf{v}_{\mathcal{L}}^{(i)}$ be the ith cyclic shift of $\mathbf{v}_{\mathcal{L}}$. Prove that

$$\mathbf{v}_{\mathcal{L}}^{(i)} \ne \mathbf{v}_{\mathcal{L}}.$$

8.32 Let $\mathcal{L}$ be a line in the two-dimensional projective geometry PG(2, 2^s). Let $\mathbf{v}_{\mathcal{L}}$ be the incidence vector of $\mathcal{L}$. For $0 < i \leq 2^{2s} + 2^s$, let $\mathbf{v}_{\mathcal{L}}^{(i)}$ be the ith cyclic shift of $\mathbf{v}_{\mathcal{L}}$. Prove that

$$\mathbf{v}_{\mathcal{L}}^{(i)} \neq \mathbf{v}_{\mathcal{L}}.$$

8.33 Prove that a cyclic shift of the incidence vector of a μ-flat in EG(m, 2^s) not passing through the origin is the incidence vector of another μ-flat in EG(m, 2^s) not passing through the origin.

8.34 Consider the cyclic product code whose component codes are the (3, 2) cyclic code generated by $g_1(X) = 1 + X$ and the (7, 4) Hamming code generated by $g_2(X) = 1 + X + X^3$. The component code C_1 is completely orthogonalizable in one step, and the component code C_2 is completely orthogonalizable in two steps. Show that the product code is completely orthogonalizable in two steps. (In general, if one component code is completely orthogonalizable in one step, and the other component code is completely orthogonalizable in L steps, the product code is completely orthogonalizable in L steps [37].)

BIBLIOGRAPHY

1. I. S. Reed, "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme," *IRE Trans.*, IT-4: 38–49, September 1954.

2. J. L. Massey, *Threshold Decoding*, MIT Press, Cambridge, 1963.

3. L. D. Rudolph, "A Class of Majority Logic Decodable Codes," *IEEE Trans. Inform. Theory*, IT-13: 305–7, April 1967.

4. T. Kasami, L. Lin, and W. W. Peterson, "Some Results on Cyclic Codes Which Are Invariant under the Affine Group and Their Applications," *Inform. Control*, 2(5 and 6): 475–96, November 1968.

5. W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2d ed. MIT Press, Cambridge, 1972.

6. S. Lin and G. Markowsky, "On a Class of One-Step Majority-Logic Decodable Cyclic Codes," *IBM J. Res. Dev.*, January 1980.

7. R. B. Yale, "Error-Correcting Codes and Linear Recurring Sequences," *Lincoln Laboratory Report*, pp. 33–77, Lincoln Labs., MIT, Cambridge, 1958.

8. N. Zierler, "On a Variation of the First-Order Reed-Muller Codes," *Lincoln Laboratory Report*, pp. 38–80, Lincoln Labs., MIT, Cambridge, 1958.

9. J. Singer, "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," *AMS Trans.*, 43: 377–85, 1938.

10. T. A. Evans and H. B. Mann, "On Simple Difference Sets," *Sankhya*, 11: 464–81, 1955.

11. L. D. Rudolph, "Geometric Configuration and Majority Logic Decodable Codes," *M.E.E. thesis*, University of Oklahoma, Norman, 1964.

Figure 9.26, and the Shannon product of these two 4-section trellises gives a 4-section trellis, as shown in Figure 9.27, which is the same as the 4-section trellis for the (8, 4, 4) RM code shown in Figure 9.17.

PROBLEMS

9.1 Consider the (6, 3) linear code generated by the following matrix:

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

a. Put this generator in trellis-oriented form.
b. Determine the active time spans of the rows in the trellis-oriented generator matrix.
c. Determine the state space dimension profile of the bit-level 6-section trellis for the code.
d. Determine the state-defining information set at each time instant.
e. Determine the input information bit at each time instant.
f. Determine the output function in each bit interval.

9.2 Construct the trellis-oriented generator matrix for the first-order RM code, RM(1, 5), of length 32.
a. Determine the active time spans of the rows.
b. Determine the state space dimension profile of the bit-level trellis for the code.
c. Determine the state-defining information set at each time instant.
d. Determine the input information bit at each time instant.
e. Determine the output function in each bit interval.

9.3 Construct the bit-level trellis for the (6, 3) code given in Problem 9.1. Label the states based on the state-defining information set using $\rho_{\max}(C)$ bits.

9.4 Find a parity-check matrix for the (6, 3) code given in Problem 9.1. Label the states of its bit-level trellis based on the parity-check matrix.

9.5 Construct the bit-level minimal trellis for the (8, 7) even-parity-check code.

9.6 Construct the bit-level trellis for the first-order RM code, RM(1, 5), of length 32. Label its states based on the state-defining information set using $\rho_{\max}(C)$ bits.

9.7 Determine the past and future subcodes of the (6, 3) linear code given in Problem 9.1 at each time instant. Determine the cosets in the partition

$$C/C_{0,4} \oplus C_{4,6}.$$

9.8 Determine the past and future subcodes of the first-order RM code, RM(1, 4), of length 16 at time instants 4, 8, and 12. Determine the cosets in the partition

$$C/C_{0,8} \oplus C_{8,16}.$$

9.9 For the first-order RM code of length 16, determine the punctured code $p_{4,8}(C)$ and punctured code $C^{tr}_{4,8}$ between time-4 and time-8. Determine the partition

$$p_{4,8}(C)/C^{tr}_{4,8}.$$

9.10 Determine the state space dimension profile of the bit-level trellis for the primitive (15,5) BCH code. Construct its bit-level trellis.

9.11 Consider the first-order RM code of length 16 given in Example 9.13. Construct a 4-section trellis for the code with section boundary locations at 0, 4, 8, 12, and 16.

9.12 Continue Problem 9.5. Construct a 4-section trellis for the first-order RM code of length 32.

9.13 Consider the first-order RM code of length 16 given in Example 9.13. Decompose the bit-level trellis into two parallel subtrellises without exceeding the maximum state space dimension.

9.14 Continue Problem 9.13. After decomposition, construct an 8-section trellis for the code.

9.15 Can the first-order RM code of length 16 be decomposed into 4 parallel subtrellises without exceeding its maximum state space dimension?

9.16 Can the bit-level trellis for the primitive (15, 5) BCH code be decomposed into two parallel subtrellises without exceeding its maximum state space dimension? If yes, decompose the trellis.

9.17 Prove that the bit-level trellis for the first-order RM code of length 16 has mirror-image symmetry.

9.18 Prove that the bit-level trellis for the first-order RM code, RM(r, m), has mirror-image symmetry.

BIBLIOGRAPHY

1. G. D. Forney, Jr., "The Viterbi Algorithm," *Proc. IEEE*, 61: 268–78, 1973.

2. A. J. Viterbi, "Error Bounds for Convolutional Codes and Asymptotically Optimum Decoding Algorithm," *IEEE Trans. Inform. Theory*, IT-13: 260–69, 1967.

3. L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate," *IEEE Trans. Inform. Theory*, IT-20: 284–87, 1974.

4. J. K. Wolf, " Efficient Maximum-Likelihood Decoding of Linear Block Codes Using a Trellis," *IEEE Trans. Inform. Theory*, IT-24: 76–80, 1978.

5. J. L. Massey, "Foundation and Methods of Channel Encoding, " in *Proc. Int. Conf. Inform. Theory and Systems*, NTG-Fachberichte, Berlin, 1978.

6. G. D. Forney Jr., "Coset Codes II: Binary Lattices and Related Codes," *IEEE Trans. Inform. Theory*, IT-34: 1152–87, 1988.

7. S. Lin, T. Kasami, T. Fujiwara, and M. P. C. Fossorier, *Trellises and Trellis-Based Decoding Algorithms for Linear Block Codes*, Kluwer Academic, Boston, Mass., 1998.

8. A. Vardy, "Trellis Structure of Codes" in *Handbook of Coding Theory*, edited by V. Pless, W. Huffman, and R. A. Brualdi, Elsevier Science, Amsterdam, 1998.

9. D. J. Muder, "Minimal Trellises for Block Codes," *IEEE Trans. Inform. Theory*, 34: 1049–53, 1988.

10. Y. Berger and Y. Be'ery, "Bounds on the Trellis Size of Linear Block Codes," *IEEE Trans. Inform. Theory*, IT-39: 203–9, 1993.

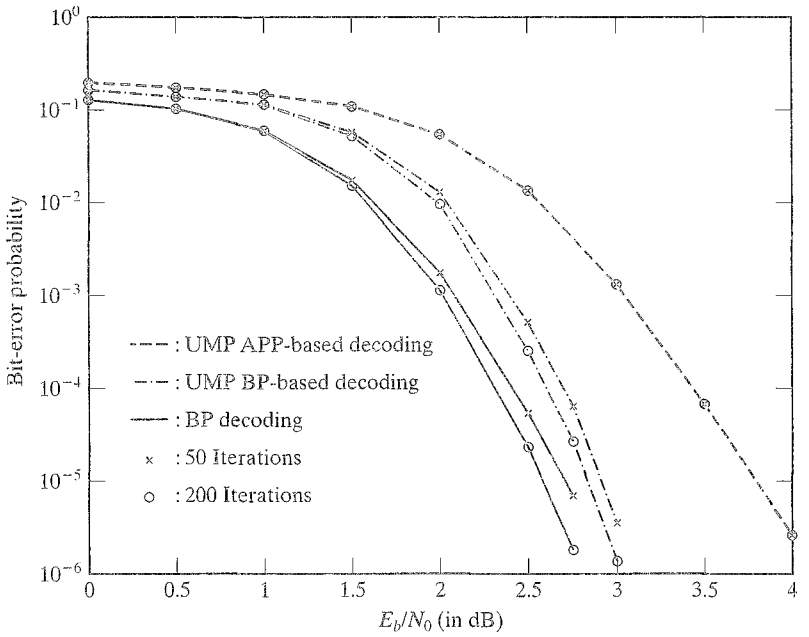


FIGURE 10.16: Error performance for iterative decoding of the (1008, 504) LDPC code with BP, UMP BP-based, and UMP APP-based decoding algorithms, and at most 50 and 200 iterations.

decoding of the (504, 252) and (1008, 504) LDPC codes (constructed by computer search), respectively, with the BP, UMP BP-based, and UMP APP-based decoding algorithms, and at most 50 and 200 iterations. The (504, 252) LDPC code has three check-sums of weight 6 orthogonal on each position, and the (1008, 504) LDPC code has four check-sums of weight 8 orthogonal on each position. We observe that the error performance of the simplified UMP BP-based algorithm is close to that of the BP algorithm and achieves a significant gain over the UMP APP-based decoding algorithm of Section 10.10.1; however, the number of required iterations is quite large, and little improvement is observed by increasing the number of iterations from 50 to 200 for BP-based decoding algorithms.

Construction of LDPC codes and various algorithms for decoding LDPC codes will be discussed in Chapter 17.

PROBLEMS

10.1 Prove the sufficient condition for optimality of a codeword given by (10.47).

10.2 Consider the value $G(\mathbf{v}_1, w_1; \mathbf{v}_2, w_1)$ given in (10.46).

a. Discuss $G(\mathbf{v}_1, w_1; \mathbf{v}_2, w_1)$ in the case where the codeword delivered by an algebraic decoder is known. What is the problem in trying to use this result for all received sequences?

b. Discuss $G(\mathbf{v}_1, w_1; \mathbf{v}_2, w_1)$ for $\mathbf{v}_1 = \mathbf{v}_2$.

10.3 GMD decoding considers only $\lfloor (d_{min} + 1)/2 \rfloor$ erasures in the $d_{min} - 1$ LRPs. Explain why not all $d_{min} - 1$ possible erasures are considered.

10.4 Consider an (n, k) binary linear code with even minimum distance d_{min}. Show that it is possible to achieve the same error performance as for the conventional Chase algorithm-2 by erasing one given position among the $\lfloor d_{min}/2 \rfloor$ least reliable positions (LRPs) of the received sequence and adding to the hard-decision decoding of the received sequence $\mathbf{r}$ all possible combinations of 0's and 1's in the remaining $\lfloor d_{min}/2 \rfloor - 1$ LRPs.

10.5 Consider an error-and-erasure algebraic decoder that successfully decodes any input sequence with t errors and s erasures satisfying $s + 2t < d_{min}$ and fails to decode otherwise. Define $S_e(a)$ as the set of candidate codewords generated by the algorithm $A_e(a)$ presented in Section 10.4. For $a = 1, \cdots, \lceil d_{min}/2 \rceil - 1$, show that $S_e(a) \subseteq S_e(a + 1)$.

10.6 In the KNIH algorithm presented in Section 10.6, show that any codeword $\mathbf{v}$ in $J(i)$ rather that the one that has the smallest correlation discrepancy with the received sequence $\mathbf{r}$ can be used for evaluating $G_i(\mathbf{v})$. Discuss the implications of this remark (advantages and drawbacks).

10.7 In the RLSD algorithm presented in Section 10.7, show that there exists at most one $(n - k)$-pattern that is not $(n - k - 1)$-eliminated.

10.8 For the RLSD algorithm presented in Section 10.7, determine the complete reduced list for the (15, 11, 3) Hamming code.

10.9 Determine the complete reduced list for the (8, 4, 4) extended Hamming code. Show that this complete list can be divided into two separate lists depending on whether the syndrome $\mathbf{s}$ is a column of the parity check matrix H. (*Hint:* Each list is composed of five distinct patterns).

10.10 In the RLSD algorithm presented in Section 10.7, prove that all $n(\mathbf{v})$-patterns with $n(\mathbf{v}) > n - k$ can be eliminated from all reduced lists. For $n(\mathbf{v}') < n(\mathbf{v})$, determine an $n(\mathbf{v}')$-pattern that justifies this elimination.

10.11 Let C and C_1 be the two codes defined in Section 10.8.1. Explain why if $\hat{\mathbf{v}}$ is the decoded codeword in C_1, then $\pi_1^{-1}\pi_2^{-1}[\hat{\mathbf{v}}]$ is simply the decoded codeword in C.

10.12 Prove that the most reliable basis and the least reliable basis are information sets of a code and its dual, respectively.

10.13 Prove that order-1 reprocessing achieves maximum likelihood decoding for the (8, 4, 4) RM code.

10.14 Which order of reprocessing achieves maximum likelihood decoding of an $(n, n - 1, 2)$ single parity-check code? Based on your answer, propose a much simpler method for achieving maximum likelihood decoding of single parity-check codes.

10.15 Describe the types of errors that can be corrected by Chase algorithm-2, but not by order-i reprocessing.

10.16 Assume that an rth-order RM code RM(r, m) is used for error control.

a. Show that all error patterns of weight at most t, as well as all error patterns of weight $t + 1$ with one error in a given position can be corrected.

b. Assuming reliability values are available at the decoder, propose a simple modification of majority-logic decoding (Reed algorithm) of RM(r, m) RM codes in which the error performance can be improved based on (a).

BIBLIOGRAPHY

1. J. G. Proakis. *Digital Communications, 3d ed.,* New York: McGraw-Hill, 1995.

2. M. P. C. Fossorier, S. Lin, and D. Rhee, "Bit Error Probability for Maximum Likelihood Decoding of Linear Block Codes and Related Soft Decision Decoding Methods," *IEEE Trans. Inform. Theory*, IT-44: 3083–90, November 1998.

$[\mathbf{v}]_l = (11, 01, 00, 00, \cdots, 00)$, even in the limit as $l \to \infty$. Note, however, that all finite-length paths in the state diagram that diverge from and remerge with the all-zero state S_0 have a weight of at least 4, and hence, $d_{free} = 4$. In this case we have a situation in which $\lim_{l\to\infty} d_l = 3 \neq d_{free} = 4$; that is, (11.168) is not satisfied.

It is characteristic of catastrophic encoders that an infinite-weight information sequence produces a finite-weight codeword. In some cases, as in the preceding example, this codeword can have a weight less than the free distance of the code, owing to the zero-output weight cycle in the state diagram. In other words, an information sequence that traverses this zero-output weight cycle forever will itself pick up infinite weight without adding to the weight of the codeword. In a noncatastrophic encoder, which contains no zero-output weight cycle other than the zero-weight cycle around the state S_0, all infinite-weight information sequences must generate infinite-weight codewords, and the minimum weight codeword always has finite length. Unfortunately, the information sequence that produces the minimum-weight codeword may be quite long in some cases, and hence the calculation of d_{free} can be a difficult task.

The best achievable d_{free} for a convolutional code with a given rate R and overall constraint length ν has not been determined in general; however, upper and lower bounds on d_{free} have been obtained using a random coding approach. These bounds are thoroughly discussed in References [16], [17], and [18]. A comparison of the bounds for nonsystematic encoders with the bounds for systematic encoders implies that more free distance is available with nonsystematic feedforward encoders of a given rate and constraint length than with systematic feedforward encoders. This observation is verified by the code construction results presented in the next two chapters and has important consequences when a code with large d_{free} must be selected for use with ML, MAP, or sequential decoding. Thus, if a systematic encoder realization is desired, it is usually better to select a nonsystematic feedforward encoder with large d_{free} and then convert it to an equivalent systematic feedback encoder.

PROBLEMS

11.1 Consider the (3, 1, 2) nonsystematic feedforward encoder with

$$\mathbf{g}^{(0)} = (1\,1\,0),$$
$$\mathbf{g}^{(1)} = (1\,0\,1),$$
$$\mathbf{g}^{(2)} = (1\,1\,1).$$

- **a.** Draw the encoder block diagram.
- **b.** Find the time-domain generator matrix $\mathbf{G}$.
- **c.** Find the codeword $\mathbf{v}$ corresponding to the information sequence $\mathbf{u} = (1\,1\,1\,0\,1)$.

11.2 Consider the (4, 3, 3) nonsystematic feedforward encoder shown in Figure 11.3.

- **a.** Find the generator sequences of this encoder.
- **b.** Find the time-domain generator matrix $\mathbf{G}$.
- **c.** Find the codeword $\mathbf{v}$ corresponding to the information sequence $\mathbf{u} = (110, 011, 101)$.

11.3 Consider the (3, 1, 2) encoder of Problem 11.1.
   a. Find the transform-domain generator matrix $\mathbb{G}(D)$.
   b. Find the set of output sequences $\mathbb{V}(D)$ and the codeword $\mathbb{v}(D)$ corresponding to the information sequence $\mathbb{u}(D) = 1 + D^2 + D^3 + D^4$.

11.4 Consider the (3, 2, 2) nonsystematic feedforward encoder shown in Figure 11.2.
   a. Find the composite generator polynomials $\mathbb{g}_1(D)$ and $\mathbb{g}_2(D)$.
   b. Find the codeword $\mathbb{v}(D)$ corresponding to the set of information sequences $\mathbb{U}(D) = [1 + D + D^3, 1 + D^2 + D^3]$.

11.5 Consider the (3, 1, 5) systematic feedforward encoder with

$$\mathbb{g}^{(1)} = (1\,0\,1\,1\,0\,1),$$
$$\mathbb{g}^{(2)} = (1\,1\,0\,0\,1\,1).$$

   a. Find the time-domain generator matrix $\mathbb{G}$.
   b. Find the parity sequences $\mathbb{v}^{(1)}$ and $\mathbb{v}^{(2)}$ corresponding to the information sequence $\mathbb{u} = (1\,1\,0\,1)$.

11.6 Consider the (3, 2, 3) systematic feedforward encoder with

$$\mathbb{g}_1^{(2)}(D) = 1 + D^2 + D^3,$$
$$\mathbb{g}_2^{(2)}(D) = 1 + D + D^3.$$

   a. Draw the controller canonical form realization of this encoder. How many delay elements are required in this realization?
   b. Draw the simpler observer canonical form realization that requires only three delay elements.

11.7 Verify the sequence of elementary row operations leading from the nonsystematic feedforward realizations of (11.34) and (11.70) to the systematic feedback realizations of (11.66) and (11.71).

11.8 Draw the observer canonical form realization of the generator matrix $\mathbb{G}'(D)$ in (11.64) and determine its overall constraint length ν.

11.9 Consider the rate $R = 2/3$ nonsystematic feedforward encoder with generator matrix

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

   a. Draw the controller canonical form encoder realization for $\mathbb{G}(D)$. What is the overall constraint length ν?
   b. Find the generator matrix $\mathbb{G}'(D)$ of the equivalent systematic feedback encoder. Is $\mathbb{G}'(D)$ realizable? If not, find an equivalent realizable generator matrix and draw the corresponding minimal encoder realization. Is this minimal realization in controller canonical form or observer canonical form? What is the minimal overall constraint length ν?

11.10 Use elementary row operations to convert the rate $R = 2/3$ generator matrix of (11.77) to systematic feedback form, and draw the minimal observer canonical form encoder realization. Find and draw a nonsystematic feedback controller canonical form encoder realization with the same number of states.

11.11 Redraw the observer canonical form realization of the (3, 2, 2) systematic feedback encoder in Figure 11.7(b) using the notation of (11.82) and the relabeling scheme of Figure 11.11.

11.12 Consider the (3, 1, 2) systematic feedback encoder shown in Figure 11.6(c). Determine the $\nu = 2$ termination bits required to return this encoder to the all-zero state when the information sequence $\mathbf{u} = (10111)$.

11.13 Consider the (4, 3, 3) nonsystematic feedforward encoder realization in controller canonical form shown in Figure 11.3.

a. Draw the equivalent nonsystematic feedforward encoder realization in observer canonical form, and determine the number of termination bits required to return this encoder to the all-zero state. What is the overall constraint length of this encoder realization?

b. Now, determine the equivalent systematic feedback encoder realization in observer canonical form, and find the number of termination bits required to return this encoder to the all-zero state. What is the overall constraint length of this encoder realization?

11.14 Consider the (2, 1, 2) nonsystematic feedforward encoder with $\mathbf{G}(D) = [1 + D^2 \;\; 1 + D + D^2]$.

a. Find the GCD of its generator polynomials.

b. Find the transfer function matrix $\mathbf{G}^{-1}(D)$ of its minimum-delay feedforward inverse.

11.15 Consider the (2, 1, 3) nonsystematic feedforward encoder with $\mathbf{G}(D) = [1 + D^2 \;\; 1 + D + D^2 + D^3]$.

a. Find the GCD of its generator polynomials.

b. Draw the encoder state diagram.

c. Find a zero-output weight cycle in the state diagram.

d. Find an infinite-weight information sequence that generates a codeword of finite weight.

e. Is this encoder catastrophic or noncatastrophic?

11.16 Find the general form of transfer function matrix $\mathbf{G}^{-1}(D)$ for the feedforward inverse of an (n, k, ν) systematic encoder. What is the minimum delay l?

11.17 Verify the calculation of the WEF in Example 11.13.

11.18 Verify the calculation of the IOWEF in Example 11.12.

11.19 Consider the (3, 1, 2) encoder of Problem 11.1.

a. Draw the state diagram of the encoder.

b. Draw the modified state diagram of the encoder.

c. Find the WEF $A(X)$.

d. Draw the augmented modified state diagram of the encoder.

e. Find the IOWEF $A(W, X, L)$.

11.20 Using an appropriate software package, find the WEF $A(X)$ for the (4, 3, 3) encoder of Figure 11.3.

11.21 Consider the equivalent systematic feedback encoder for Example 11.1 obtained by dividing each generator polynomial by $\mathbf{g}^{(0)}(D) = 1 + D^2 + D^3$.

a. Draw the augmented modified state diagram for this encoder.

b. Find the IRWEF $A(W, Z)$, the two lowest input weight CWEFs, and the WEF $A(X)$ for this encoder.

c. Compare the results obtained in (b) with the IOWEF, CWEFs, and WEF computed for the equivalent nonsystematic feedforward encoder in Example 11.1.

11.22 Verify the calculation of the IOWEF given in (11.124) for the case of a terminated convolutional encoder.

11.23 Consider the equivalent nonsystematic feedforward encoder for Example 11.14 obtained by multiplying $\mathbf{G}(D)$ in (11.140) by $\mathbf{g}^{(0)}(D) = 1 + D + D^2$.

a. Draw the augmented modified state diagram for this encoder.
b. Find the IOWEF $A(W, X, L)$, the three lowest input weight CWEFs, and the WEF $A(X)$ for this encoder.
c. Compare the results obtained in (b) with the IRWEF, CWEFs, and WEF computed for the equivalent systematic feedback encoder in Example 11.14.

11.24 In Example 11.14, verify all steps leading to the calculation of the bit WEF in (11.154).

11.25 Consider the (2, 1, 2) systematic feedforward encoder with $\mathbb{G}(D) = [1 \;\; 1 + D^2]$.
a. Draw the augmented modified state diagram for this encoder.
b. Find the IRWEF $A(W, Z, L)$, the three lowest input weight CWEFs, and the WEF $A(X)$ for this encoder.

11.26 Recalculate the IOWEF $A(W, X, L)$ in Example 11.12 using the state variable approach of Example 11.14.

11.27 Recalculate the WEF $A(X)$ in Example 11.13 using the state variable approach of Example 11.14.

11.28 Consider the (3, 1, 2) code generated by the encoder of Problem 11.1.
a. Find the free distance d_{free}.
b. Plot the complete CDF.
c. Find the minimum distance d_{min}.

11.29 Repeat Problem 11.28 for the code generated by the encoder of Problem 11.15.

11.30 a. Prove that the free distance d_{free} is independent of the encoder realization, i.e., it is a code property.
b. Prove that the CDF d_l is independent of the encoder realization; that is, it is a code property. (Assume that the $k \times n$ submatrix $\mathbb{G}_0$ has full rank.)

11.31 Prove that for noncatastrophic encoders

$$\lim_{l \to \infty} d_l = d_{free}.$$

BIBLIOGRAPHY

1. P. Elias, "Coding for Noisy Channels," *IRE Conv. Rec., p. 4*: 37–47, 1955.

2. J. M. Wozencraft and B. Reiffen, *Sequential Decoding*, MIT Press, Cambridge, 1961.

3. J. L. Massey, *Threshold Decoding*. MIT Press, Cambridge, 1963.

4. A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," *IEEE Trans. Inform. Theory*, IT-13: 260–69, April 1967.

5. L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal Decoding of Linear Codes for Minimal Symbol Error Rate," *IEEE Trans. Inform. Theory*, IT-20: 284–87, March 1974.

6. G. Ungerboeck and I. Csajka, "On Improving Data-Link Performance by Increasing the Channel Alphabet and Introducing Sequence Coding," in *IEEE International Symposium on Information Theory (ISIT 1976) Book of Abstracts*, p. 53, Ronneby, Sweden, June 1976.

We see from Table 12.6 that, in general, for a given rate R_{tb} and constraint length ν, the minimum distance d_{min} of the best block (tail-biting convolutional) code increases, or the number of nearest neighbors decreases, as the information block length K^* increases. Once K^* reaches a certain value, though, the minimum distance d_{min} of the best block (tail-biting convolutional) code is limited by the free distance d_{free} of the best terminated convolutional code with constraint length ν, and no further increase in d_{min} is possible; however, the number of nearest neighbors $A_{d_{min}}$ continues to grow linearly with K^*. Once this limit is reached, the generator sequences $\mathbf{g}^{(j)}$ (parity-check sequences $\mathbf{h}^{(j)}$ in the rate $R_{tb} = 2/3$ case) and the minimum distance d_{min} stay the same, and in Table 12.6 we simply list the growth rate of $A_{d_{min}}$. In other words, for a given R_{tb} and ν, block (tail-biting convolutional) codes improve as K^* increases up to a point, and then the codes get worse. Similarly, we can see from Table 12.6 that for a given R_{tb} and K^*, block (tail-biting convolutional) codes improve as ν increases up to a point, and then d_{min} and $A_{d_{min}}$ remain the same. Thus, the best block (tail-biting convolutional) codes are obtained by choosing the length K^* or the constraint length ν only as large as is needed to achieve the desired combination of d_{min} and $A_{d_{min}}$. It is worth noting that many of the best binary block codes can be represented as tail-biting convolutional codes, and thus they can be decoded using the ML (Viterbi) or MAP (BCJR) soft-decision decoding algorithms (see Problem 12.39).

PROBLEMS

12.1 Draw the trellis diagram for the (3, 2, 2) encoder in Example 11.2 and an information sequence of length $h = 3$ blocks. Find the codeword corresponding to the information sequence $\mathbf{u} = (11, 01, 10)$. Compare the result with (11.16) in Example 11.2.

12.2 Show that the path $\mathbf{v}$ that maximizes $\sum_{l=0}^{N-1} \log P(r_l|v_l)$ also maximizes $\sum_{l=0}^{N-1} c_2[\log P(r_l|v_l) + c_1]$, where c_1 is any real number and c_2 is any positive real number.

12.3 Find the integer metric table for the DMC of Figure 12.3 when $c_1 = 1$ and $c_2 = 10$. Use the Viterbi algorithm to decode the received sequence $\mathbf{r}$ of Example 12.1 with this integer metric table and the trellis diagram of Figure 12.1. Compare your answer with the result of Example 12.1.

12.4 Consider a binary-input, 8-ary output DMC with transition probabilities $P(r_l|v_l)$ given by the following table:

$v_l^{(j)}$ \ $r_l^{(j)}$	$\mathbb{0}_1$	$\mathbb{0}_2$	$\mathbb{0}_3$	$\mathbb{0}_4$	$\mathbb{1}_4$	$\mathbb{1}_3$	$\mathbb{1}_2$	$\mathbb{1}_1$
0	0.434	0.197	0.167	0.111	0.058	0.023	0.008	0.002
1	0.002	0.008	0.023	0.058	0.111	0.167	0.197	0.434

Find the metric table and an integer metric table for this channel.

12.5 Consider the (2, 1, 3) encoder of Figure 11.1 with

$$\mathbf{G}(D) = [1 + D^2 + D^3 \quad 1 + D + D^2 + D^3]$$

a. Draw the trellis diagram for an information sequence of length $h = 4$.

b. Assume a codeword is transmitted over the DMC of Problem 12.4. Use the Viterbi algorithm to decode the received sequence $\mathbf{r} = (1_2 1_1, 1_2 0_1, 0_3 0_1, 0_1 1_3, 1_2 0_2, 0_3 1_1, 0_3 0_2)$.

12.6 The DMC of Problem 12.4 is converted to a BSC by combining the soft-decision outputs 0_1, 0_2, 0_3, and 0_4 into a single hard-decision output 0, and the soft-decision outputs 1_1, 1_2, 1_3, and 1_4 into a single hard-decision output 1. A codeword from the code of Problem 12.5 is transmitted over this channel. Use the Viterbi algorithm to decode the hard-decision version of the received sequence in Problem 12.5 and compare the result with Problem 12.5.

12.7 A codeword from the code of Problem 12.5 is transmitted over a continuous-output AWGN channel. Use the Viterbi algorithm to decode the (normalized by $\sqrt{E_S}$) received sequence $\mathbf{r} = (+1.72, +0.93, +2.34, -3.42, -0.14, -2.84, -1.92, +0.23, +0.78, -0.63, -0.05, +2.95, -0.11, -0.55)$.

12.8 Consider a binary-input, continuous-output AWGN channel with signal-to-noise ratio $E_s/N_0 = 0$ dB.

a. Sketch the conditional pdf's of the (normalized by $\sqrt{E_s}$) received signal r_l given the transmitted bits $v_l = \pm 1$.

b. Convert this channel into a binary-input, 4-ary output symmetric DMC by placing quantization thresholds at the values $r_l = -1, 0$, and $+1$, and compute the transition probabilities for the resulting DMC.

c. Find the metric table and an integer metric table for this DMC.

d. Repeat parts (b) and (c) using quantization thresholds $r_l = -2, 0$, and $+2$.

12.9 Show that (12.21) is an upper bound on P_d for d even.

12.10 Consider the (2, 1, 3) encoder of Problem 12.5. Evaluate the upper bounds on event-error probability (12.25) and bit-error probability (12.29) for a BSC with transition probability

a. $p = 0.1$,

b. $p = 0.01$.

(*Hint*: Use the WEFs derived for this encoder in Example 11.12.)

12.11 Repeat Problem 12.10 using the approximate expressions for $P(E)$ and $P_b(E)$ given by (12.26) and (12.30).

12.12 Consider the (3, 1, 2) encoder of (12.1). Plot the approximate expression (12.36) for bit-error probability $P_b(E)$ on a BSC as a function of E_b/N_0 in decibels. Also plot on the same set of axes the approximate expression (12.37) for $P_b(E)$ without coding. The *coding gain* (in decibels) is defined as the difference between the E_b/N_0 ratio needed to achieve a given bit-error probability with coding and without coding. Plot the coding gain as a function of $P_b(E)$. Find the value of E_b/N_0 for which the coding gain is 0 dB, that is, the *coding threshold*.

12.13 Repeat Problem 12.12 for an AWGN channel with unquantized demodulator outputs, that is, a continuous-output AWGN channel, using the approximate expression for $P_b(E)$ given in (12.46).

12.14 Consider using the (3, 1, 2) encoder of (12.1) on the DMC of Problem 12.4. Calculate an approximate value for the bit-error probability $P_b(E)$ based on the bound of (12.39b). Now, convert the DMC to a BSC, as described in Problem 12.6, compute an approximate value for $P_b(E)$ on this BSC using (12.29), and compare the two results.

12.15 Prove that the rate $R = 1/2$ quick-look-in encoders defined by (12.58) are noncatastrophic.

12.16 Consider the following two nonsystematic feedforward encoders: (1) the encoder for the (2, 1, 7) optimum code listed in Table 12.1(c) and (2) the encoder for the (2, 1, 7) quick-look-in code listed in Table 12.2. For each of these codes find

a. the soft-decision asymptotic coding gain γ;

b. the approximate event-error probability on a BSC with $p = 10^{-2}$;

c. the approximate bit-error probability on a BSC with $p = 10^{-2}$;

d. the error probability amplification factor A.

12.17 Using trial-and-error methods, construct a (2, 1, 7) systematic feedforward encoder with maximum d_{free}. Repeat Problem 12.16 for this code.

12.18 Consider the (15,7) and (31,16) cyclic BCH codes. For each of these codes find

a. the polynomial generator matrix and a lower bound on d_{free} for the rate $R = 1/2$ convolutional code derived from the cyclic code using Construction 12.1;

b. the polynomial generator matrix and a lower bound on d_{free} for the rate $R = 1/4$ convolutional code derived from the cyclic code using Construction 12.2.

(*Hint:* d_h is at least one more than the maximum number of consecutive powers of α that are roots of $\mathbf{h}(X)$.)

12.19 Consider the (2, 1, 1) systematic feedforward encoder with $\mathbf{G}(D) = [1 \quad 1 + D]$.

a. For a continuous-output AWGN channel and a truncated Viterbi decoder with path memory $\tau = 2$, decode the received sequence $\mathbf{r} = (+1.5339, +0.6390, -0.6747, -3.0183, +1.5096, +0.7664, -0.4019, +0.3185, +2.7121, -0.7304, +1.4169, -2.0341, +0.8971, -0.3951, +1.6254, -1.1768, +2.6954, -1.0575)$ corresponding to an information sequence of length $h = 8$. Assume that at each level the survivor with the best metric is selected and that the information bit τ time units back on this path is decoded.

b. Repeat (a) for a truncated Viterbi decoder with path memory $\tau = 4$.

c. Repeat (a) for a Viterbi decoder without truncation.

d. Are the final decoded paths the same in all cases ? Explain.

12.20 Consider the (3, 1, 2) encoder of Problem 11.19.

a. Find $A_1(W, X, L)$, $A_2(W, X, L)$, and $A_3(W, X, L)$.

b. Find τ_{min}.

c. Find $d(\tau)$ and $A_{d(\tau)}$ for $\tau = 0, 1, 2, \cdots, \tau_{min}$.

d. Find an expression for $\lim_{\tau \to \infty} d(\tau)$.

12.21 A codeword from the trellis diagram of Figure 12.1 is transmitted over a BSC. To determine correct symbol synchronization, each of the three 21-bit subsequences of the sequence

$$\mathbf{r} = 0\,1\,1\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1$$

must be decoded, where the two extra bits in $\mathbf{r}$ are assumed to be part of a preceding and/or a succeeding codeword. Decode each of these subsequences and determine which one is most likely to be the correctly synchronized received sequence.

12.22 Consider the binary-input, continuous-output AWGN channel of Problem 12.8.

a. Using the optimality condition of (12.84), calculate quantization thresholds for DMCs with $Q = 2, 4$, and 8 output symbols. Compare the thresholds obtained for $Q = 4$ with the values used in Problem 12.8.

b. Find the value of the Bhattacharyya parameter D_0 for each of these channels and for a continuous-output AWGN channel.

c. Fixing the signal energy $\sqrt{E_s} = 1$ and allowing the channel SNR E_s/N_0 to vary, determine the increase in the SNR required for each of the DMCs to achieve

the same value of D_0 as the continuous-output channel. This SNR difference is called the *decibel loss* associated with receiver quantization. (*Note:* Changing the SNR also changes the quantization thresholds.)

(*Hint:* You will need to write a computer program to solve this problem.)

12.23 Verify that the two expressions given in (12.89) for the modified metric used in the SOVA algorithm are equivalent.

12.24 Define $L(r) = \ln \lambda(r)$ as the log-likelihood ratio, or L-value, of a received symbol r at the output of an unquantized binary input channel. Show that the L-value of an AWGN channel with binary inputs $\pm\sqrt{E_s}$ and SNR E_s/N_0 is given by

$$L(r) = (4\sqrt{E_s}/N_0)r.$$

12.25 Verify that the expressions given in (12.98) are correct, and find the constant c.

12.26 Consider the encoder, channel, and received sequence of Problem 12.19.

a. Use the SOVA with full path memory to produce a soft output value for each decoded information bit.

b. Repeat (a) for the SOVA with path memory $\tau = 4$.

12.27 Derive the expression for the backward metric given in (12.117).

12.28 Verify the derivation of (12.123) and show that $A_l = e^{-\frac{L_a(u_l)/2}{1+e^{-L_a(u_l)}}}$ is independent of the actual value of u_l.

12.29 Derive the expressions for the $\max^*(x, y)$ and $\max^*(x, y, z)$ functions given in (12.127) and (12.131), respectively.

12.30 Consider the encoder and received sequence of Problem 12.19.

a. For an AWGN channel with $E_s/N_0 = 1/2$ (−3 dB), use the log-MAP version of the BCJR algorithm to produce a soft output value for each decoded information bit. Find the decoded information sequence $\hat{\mathbf{u}}$.

b. Repeat (a) using the Max-log-MAP algorithm.

12.31 Repeat Problem 12.5 using the probability-domain version of the BCJR algorithm.

12.32 Show that using the normalized forward and backward metrics $A_l(s)$ and $B_l(s')$ instead of $\alpha_l(s)$ and $\beta_l(s')$, respectively, to evaluate the joint pdf's in (12.115) has no effect on the APP L-values computed using (12.111).

12.33 Verify all the computations leading to the determination of the final APP L-values in Example 12.9.

12.34 Repeat Example 12.9 for the case when the DMC is converted to a BSC, as described in Problem 12.6, and the received sequence $\mathbf{r}$ is replaced by its hard-decision version. Compare the final APP L-values in the two cases.

12.35 Consider an 8-state rate $R = 1/2$ mother code with generator matrix

$$\mathbb{G}(D) = [1 + D + D^3 \quad 1 + D^2 + D^3].$$

Find puncturing matrices $\mathbb{P}$ for the rate $R = 2/3$ and $R = 3/4$ punctured codes that give the best free distances. Compare your results with the free distances obtained using the 8-state mother code in Table 12.4.

12.36 Prove that the subcode corresponding to any nonzero state S_i, $i \neq 0$, in a tail-biting convolutional code is a coset of the subcode corresponding to the all-zero state S_0.

12.37 For the rate $R = 1/2$ feedback encoder tail-biting trellis in Figure 12.24(b), determine the parameters d_{min} and $A_{d_{min}}$ for information block lengths $K^* = 7, 8$, and 9. Is it possible to form a tail-biting code in each of these cases?

12.38 Verify that the row space of the tail-biting generator matrix in (12.164) is identical to the tail-biting code of Table 12.5(a).

12.39 Consider the rate $R = 4/8$, constraint length $\nu = 4$ feedforward convolutional encoder with generator matrix

$$\mathbf{G}(D) = \begin{bmatrix} 1+D & 0 & 1 & 0 & 1+D & 1 & 1 & 1 \\ 0 & 1+D & 1 & 1 & D & 1+D & 1 & 0 \\ D & D & 1+D & 0 & 0 & D & 1+D & 1 \\ 0 & D & 0 & 1+D & D & D & D & 1+D \end{bmatrix}$$

a. Draw the controller canonical form encoder diagram.
b. Draw an $h = 3$ ($K^* = 12$), 16-state tail-biting trellis for this encoder.
c. Find the tail-biting generator matrix $\mathbf{G}_b^{tb}$ for the resulting (24, 12) tail-biting code.
d. Show that this code has $d_{min} = 8$ and is equivalent to the (24, 12) extended Golay code.
(*Note:* The convolutional code generated by $\mathbf{G}(D)$ is called the *Golay convolutional code.*)

BIBLIOGRAPHY

1. A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," *IEEE Trans. Inform. Theory*, IT-13: 260–69, April 1967.

2. J. K. Omura, "On the Viterbi Decoding Algorithm," *IEEE Trans. Inform. Theory*, IT-15: 177–79, January 1969.

3. G. D. Forney, Jr., "The Viterbi Algorithm," *Proc. IEEE*, 61: 268–78, March 1973.

4. G. D. Forney, Jr., "Convolutional Codes II: Maximum Likelihood Decoding," *Inform. Control*, 25: 222–66, July 1974.

5. L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate," *IEEE Trans. Inform. Theory*, IT-20: 284–87, March 1974.

6. P. L. McAdam, L. R. Welch, and C. L. Weber, "M.A.P. Bit Decoding of Convolutional Codes," in *Book of Abstracts IEEE International Symposium on Information Theory*, p. 91, Asilomar, Calif., February 1972.

7. L. N. Lee, "Real-Time Minimal-Bit-Error Probability Decoding of Convolutional Codes," *IEEE Trans. Commun.*, COM-22: 146–51, February 1974.

8. C. R. P. Hartmann and L. D. Rudolph, "An Optimum Symbol-by-Symbol Decoding Rule for Linear Codes," *IEEE Trans. Inform. Theory*, IT-22: 514–17, September 1976.

9. J. Hagenauer and P. Hoeher, "A Viterbi Decoding Algorithm with Soft-Decision Outputs and Its Applications," *Proc. IEEE Global Conference on Communications*, pp. 1680–86, Dallas, Tex., November 1989.

This code has $d_{min} = 9$, is completely orthogonalizable, and has error-correcting capability $t_{FB} = t_{ML} = \lfloor J/2 \rfloor = 4$.

Note that (n, k, m) orthogonalizable codes can achieve a given majority-logic error-correcting capability t_{ML} with a smaller memory order m than self-orthogonal codes, owing to the added flexibility available in using sums of syndrome bits to form orthogonal parity checks for orthogonalizable codes. The major disadvantage of orthogonalizable codes is that they do not possess the automatic resynchronization property that limits error propagation when used with feedback decoding.

PROBLEMS

13.1 Consider the (2, 1, 3) encoder with

$$\mathbb{G}(D) = [1 + D^2 + D^3 \quad 1 + D + D^2 + D^3].$$

a. Draw the code tree for an information sequence of length $h = 4$.
b. Find the codeword corresponding to the information sequence $\mathbb{u} = (1\ 0\ 0\ 1)$.

13.2 For a binary-input, Q-ary output symmetric DMC with equally likely input symbols, show that the output symbol probabilities satisfy (13.7).

13.3 Consider the (2, 1, 3) encoder of Problem 13.1.
a. For a BSC with $p = .045$, find an integer metric table for the Fano metric.
b. Decode the received sequence

$$\mathbb{r} = (1\,1,\ 0\,0,\ 1\,1,\ 0\,0,\ 0\,1,\ 1\,0,\ 1\,1)$$

using the stack algorithm. Compare the number of decoding steps with the number required by the Viterbi algorithm.
c. Repeat (b) for the received sequence

$$\mathbb{r} = (1\,1,\ 1\,0,\ 0\,0,\ 0\,1,\ 1\,0,\ 0\,1,\ 0\,0).$$

Compare the final decoded path with the results of Problem 12.6, where the same received sequence is decoded using the Viterbi algorithm.

13.4 Consider the (2, 1, 3) encoder of Problem 13.1.
a. For the binary-input, 8-ary output DMC of Problem 12.4, find an integer metric table for the Fano metric. (*Hint*: Scale each metric by an appropriate factor and round to the nearest integer.)
b. Decode the received sequence

$$\mathbb{r} = (1_2 1_1,\ 1_2 0_1,\ 0_3 0_1,\ 0_1 1_3,\ 1_2 0_2,\ 0_3 1_1,\ 0_3 0_2)$$

using the stack algorithm. Compare the final decoded path with the result of Problem 12.5(b), where the same received sequence is decoded using the Viterbi algorithm.

13.5 Consider the (2, 1, 3) encoder of Problem 13.1. For a binary-input, continuous-output AWGN channel with $E_s/N_0 = 1$, use the stack algorithm and the AWGN channel Fano metric from (13.16) to decode the received sequence $\mathbb{r} = (+1.72, +0.93, +2.34, -3.42, -0.14, -2.84, -1.92, +0.23, +0.78, -0.63, -0.05, +2.95, -0.11, -0.55)$. Compare the final decoded path with the result of Problem 12.7, where the same received sequence is decoded using the Viterbi algorithm.

13.6 Repeat parts (b) and (c) of Problem 13.3 with the size of the stack limited to 10 entries. When the stack is full, each additional entry causes the path on the bottom of the stack to be discarded. What is the effect on the final decoded path?

13.7 a. Repeat Example 13.5 using the stack-bucket algorithm with a bucket quantization interval of 5. Assume the bucket intervals are $\cdots +4$ to 0, -1 to -5, -6 to -10, $\cdots$.

b. Repeat part (a) for a quantization interval of 9, where the bucket intervals are $\cdots +8$ to 0, -1 to -9, -10 to -18, $\cdots$.

13.8 Repeat Example 13.7 for the Fano algorithm with threshold increments of $\Delta = 5$ and $\Delta = 10$. Compare the final decoded path and the number of computations to the results of Examples 13.7 and 13.8. Also compare the final decoded path with the results of the stack-bucket algorithm in Problem 13.7.

13.9 Using a computer program, verify the results of Figure 13.13, and plot ρ as a function of E_b/N_0 (dB) for $R = 1/5$ and $R = 4/5$.

13.10 Show that the Pareto exponent ρ satisfies $\lim_{R \to 0} \rho = \infty$ and $\lim_{R \to C} \rho = 0$ for fixed channel transition probabilities. Also show that $\partial R/\partial \rho < 0$.

13.11 a. For a BSC with crossover probability p, plot both the channel capacity C and the cut-off rate R_0 as functions of p. (*Note*: $C = 1 + p \log_2 p + (1 - p) \log_2 (1 - p)$.)

b. Repeat part (a) by plotting C and R_0 as functions of the SNR E_b/N_0. What is the SNR difference required to make $C = R_0 = 1/2$?

13.12 a. Calculate R_0 for the binary-input, 8-ary output DMC of Problem 12.4.

b. Repeat Example 13.9 for the DMC of part (a) and a code rate of $R = 1/2$. (*Hint:* Use a computer program to find ρ from (13.23) and (13.24).)

c. For the value of ρ calculated in part (b), find the buffer size B needed to guarantee an erasure probability of 10^{-3} using the values of L, A, and μ given in Example 13.9.

13.13 a. Sketch $P_{erasure}$ versus E_b/N_0 for a rate $R = 1/2$ code on a BSC using the values of L, A, μ, and B given in Example 13.9.

b. Sketch the required buffer size B to guarantee an erasure probability of 10^{-3} as a function of E_b/N_0 for a rate $R = 1/2$ code on a BSC using the values of L, A, and μ given in Example 13.9. (*Hint:* ρ can be found as a function of E_b/N_0 using the results of Problem 13.9.)

13.14 Repeat Problem 13.4 using the integer metric tables of Figures 13.14(a) and (b). Note any changes in the final decoded path or the number of decoding steps.

13.15 For a BSC with crossover probability p, plot both the computational cutoff rate R_0 from (13.27) and R_{max} from (13.35) as functions of p.

13.16 Find the complete CDFs of the $(2, 1, 3)$ optimum free distance code in Table 12.1(c) and the $(2, 1, 3)$ quick-look-in code in Table 12.2. Which code has the superior distance profile?

13.17 Show that for the BSC, the received sequence $\mathbf{r}$ is a codeword if and only if the error sequence $\mathbf{e}$ is a codeword.

13.18 Using the definition of the $\mathbf{H}$ matrix for rate $R = 1/2$ systematic codes given by (13.42), show that (13.41) and (13.46) are equivalent.

13.19 Draw the complete encoder/decoder block diagram for Example 13.11.

13.20 Consider the $(2, 1, 11)$ systematic code with

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

a. Find the parity-check matrix $\mathbf{H}$.

b. Write equations for the syndrome bits $s_0, s_1, \cdots, s_{11}$ in terms of the channel error bits.

c. Write equations for the modified syndrome bits $s'_l, s'_{l+1}, \cdots, s'_{l+11}$, assuming that the effect of error bits prior to time unit l has been removed by feedback.

13.21 Consider the (3, 2, 13) code of Example 13.12 and the (3, 1, 4) code of Example 13.13.
a. Find the generator matrix $\mathbb{G}(D)$.
b. Find the parity-check matrix $\mathbb{H}(D)$.
c. Show that in each case $\mathbb{G}(D)\mathbb{H}^T(D) = \mathbb{0}$.

13.22 Consider the (3, 2, 13) code of Example 13.12.
a. Write equations for the unmodified syndrome bits $s_l, s_{l+1}, \cdots, s_{l+13}$ that include the effect of error bits prior to time unit l (assume $l \geq 13$).
b. Find a set of orthogonal parity checks for both $e_l^{(0)}$ and $e_l^{(1)}$ from the unmodified syndrome equations.
c. Determine the resulting majority-logic error-correcting capability t_{ML} and the effective decoding length n_E and compare these values with those in Example 13.12.
d. Draw the block diagram of the decoder. (Note that in this case the decoding estimates are not fed back to modify the syndrome. This alternative to feedback decoding is called *definite decoding*.)

13.23 Find a rate $R = 1/2$ nonsystematic feedforward encoder with the smallest possible value of m such that $J = 4$ orthogonal parity checks can be formed on the error bits $e_0^{(0)}$ and $e_0^{(1)}$.

13.24 Prove (13.65).

13.25 Prove (13.66).

13.26 Prove that if the weighting factors w_i, $i = 0, 1, \cdots, J$, are calculated using (13.64) and (13.67) for a BSC with crossover probability p, the APP threshold decoding rule is equivalent to the majority-logic decoding rule only if all J orthogonal check-sums include the same number of bits, that is, only if $n_1 = n_2 = \cdots = n_J$.

13.27 Consider an (n, k, m) convolutional code with minimum distance $d_{min} = 2t_{FB} + 1$. Prove that there is at least one error sequence $\mathbb{e}$ with weight $t_{FB} + 1$ in its first $(m + 1)$ blocks for which a feedback decoder will decode $\mathbb{u}_0$ incorrectly.

13.28 Consider the (2, 1, 11) code of Problem 13.20.
a. Find the minimum distance d_{min}.
b. Is this code self-orthogonal?
c. Find the maximum number of orthogonal parity checks that can be formed on $e_0^{(0)}$.
d. Is this code completely orthogonalizable?

13.29 Consider the (3, 1, 3) nonsystematic feedforward encoder with $\mathbb{G}_{ns}(D) = [1 + D + D^3 \quad 1 + D^3 \quad 1 + D + D^2]$.
a. Following the procedure in Example 13.14, convert this code to a (3, 1, 3) systematic feedforward encoder with the same d_{min}.
b. Find the generator matrix $\mathbb{G}_s(D)$ of the systematic feedforward encoder.
c. Find the minimum distance d_{min}.

13.30 Consider the (2, 1, 6) code of Example 13.15.
a. Estimate the bit-error probability $P_b(E)$ of a feedback decoder with error-correcting capability t_{FB} on a BSC with small crossover probability p.
b. Repeat (a) for a feedback majority-logic decoder with error-correcting capability t_{ML}.
c. Compare the results of (a) and (b) for $p = 10^{-2}$.

13.31 Repeat Problem 13.30 for the (2, 1, 5) code of Example 13.16.

13.32 Find and compare the memory orders of the following codes:

a. the best rate $R = 1/2$ self-orthogonal code with $d_{min} = 9$.
b. the best rate $R = 1/2$ orthogonalizable code with $d_{min} = 9$.
c. the best rate $R = 1/2$ systematic code with $d_{min} = 9$.
d. the best rate $R = 1/2$ nonsystematic code with $d_{free} = 9$.

13.33 Consider an $(n, n-1, m)$ self-orthogonal code with J_j orthogonal check-sums on $e_0^{(j)}$, $j = 0, 1, \cdots, n-2$. Show that $d_{min} = J + 1$, where $J \triangleq \min_{(0 \le j \le n-2)} J_j$.

13.34 Consider the $(2, 1, 17)$ self-orthogonal code in Table 13.2(a).
a. Form the orthogonal check-sums on information error bit $e_0^{(0)}$.
b. Draw the block diagram of the feedback majority-logic decoder for this code.

13.35 Consider an $(n, 1, m)$ systematic code with generator polynomials $\mathbf{g}^{(j)}(D)$, $j = 1, 2, \cdots, n-1$. Show that the code is self-orthogonal if and only if the positive difference sets associated with each generator polynomial are full and disjoint.

13.36 Find the effective decoding length n_E for the $(3, 1, 13)$ code of Example 13.19.

13.37 Consider the $(2, 1, 11)$ orthogonalizable code in Table 13.3(a).
a. Form the orthogonal check-sums on information error bit $e_0^{(0)}$.
b. Draw the block diagram of the feedback majority-logic decoder for this code.

BIBLIOGRAPHY

1. J. M. Wozencraft, "Sequential Decoding for Reliable Communication," *IRE Conv. Rec.* 5 (pt. 2): 11–25, 1957.

2. J. M. Wozencraft and B. Reiffen, *Sequential Decoding*. MIT Press, Cambridge, 1961.

3. R. M. Fano, "A Heuristic Discussion of Probabilistic Decoding," *IEEE Trans. Inform. Theory*, IT-9: 64–74, April 1963.

4. K. Zigangirov, "Some Sequential Decoding Procedures," *Prob. Peredachi Inform.*, 2: 13–25, 1966.

5. F. Jelinek, "A Fast Sequential Decoding Algorithm Using a Stack," *IBM J. Res. Dev.*, 13: 675–85, November 1969.

6. J. L. Massey, *Threshold Decoding*. MIT Press, Cambridge, 1963.

7. J. L. Massey, "Variable-Length Codes and the Fano Metric," *IEEE Trans. Inform. Theory*, IT-18: 196–98, January 1972.

8. J. M. Geist, "Search Properties of Some Sequential Decoding Algorithms," *IEEE Trans. Inform. Theory*, IT-19: 519–26, July 1973.

9. J. M. Geist, "An Empirical Comparison of Two Sequential Decoding Algorithms," *IEEE Trans. Commun. Technol.*, COM-19: 415–19, August 1971.

10. J. E. Savage, "Sequential Decoding—The Computation Problem," *Bell Syst. Tech. J.*, 45: 149–75, January 1966.

11. I. M. Jacobs and E. R. Berlekamp, "A Lower Bound to the Distribution of Computation for Sequential Decoding," *IEEE Trans. Inform. Theory*, IT-13: 167–74, April 1967.

known. Hence,

$$\begin{aligned}\log(e^{\delta_1} + \cdots + e^{\delta_i}) &= \log(\Delta + e^{\delta_i}) \\ &= \max\{\log \Delta, \delta_i\} + f_c(|\log \Delta - \delta_i|),\end{aligned} \tag{14.126}$$

with $\Delta = e^{\delta_1} + \cdots + e^{\delta_{i-1}}$. Based on this recursion, we modify the Max-log-MAP algorithm by using simple correction functions. This algorithm, called the *log-MAP algorithm* [31], gives the same error performance as the MAP algorithm but is easier to implement. Each correction term needs an additional one-dimensional lookup table and two additions based on (14.125). Consequently, the log-MAP algorithm requires only additions and comparisons to compute the LLRs.

The storage requirement for the log-MAP algorithm is the same as those for the MAP and Max-log-MAP algorithms, assuming the storage of the lookup tables is negligible.

Consider the computational complexity of the log-MAP algorithm. Because two extra additions are required per comparison to calculate $f_c(\cdot)$ in (14.125), a total of $N_a^i(\gamma) + 3N_c^i(\gamma)$, $N_a^i(\alpha) + 3N_c^i(\alpha)$, $N_a^i(\beta) + 3N_a^i(\beta)$, and $N_a^i(\tilde{L}) + 3N_c^i(\tilde{L})$ addition-equivalent operations are required to compute $\log \gamma$'s, $\log \alpha$'s, $\log \beta$'s, and LLRs in T_i, respectively, where $N_a^i()$'s and $N_c^i()$'s are the numbers of additions and comparisons evaluated for the Max-log-MAP algorithm.

Table 14.5 gives optimum sectionalizations (in terms of minimizing the number of addition-equivalent operations) of trellises for some RM codes with the log-MAP decoding. For comparison, the computational complexities and storage requirements of these codes based on bit-level trellises are also included. We also see that proper sectionalization reduces computational complexity and storage requirements for the log-MAP algorithm.

PROBLEMS

14.1 Suppose the (8, 4) RM code is decoded with the Viterbi algorithm. Determine the number of real operations (additions and comparisons) required for the following trellises:
- a. The eight-section bit-level trellis.
- b. The uniform four-section (two-bits per section) trellis shown in Figure 9.17.
- c. Optimum sectionalization based on the Lafourcade–Vardy algorithm.

14.2 Suppose the (8, 4) RM code is decoded with the differential Viterbi decoding algorithm based on the uniform 4-section trellis of the code. Determine the number of real operations required to decode the code.

14.3 The first-order RM code of length 16 is a (16, 5) linear code with a minimum distance of 8. Decode this code with the Viterbi algorithm. Determine the number of real operations required for the decoding based on the following trellis sectionalizations:
- a. The 16-section bit-level trellis.
- b. The uniform eight-section trellis.
- c. The uniform four-section trellis.
- d. Optimum sectionalization based on the Lafourcade–Vardy algorithm.

14.4 Decode the (16, 5) first-order RM code with the differential Viterbi decoding algorithm based on the uniform four-section trellis. For each section, determine the parallel components, the set of branches leaving a state at the left end of a parallel component, and the set of branches entering a state at the right end of

a component. Decompose each component into 2-state butterflies with doubly complementary structure. Determine the total number of real operations required to decode the code.

14.5 Decode the (8, 4) RM code with the trellis-based recursive MLD algorithm. At the beginning (or bottom) of the recursion, the code is divided into four sections, and each section consists of 2 bits. The composite path metric table for each of these basic sections is constructed directly. Devise a recursion procedure to combine these metric tables to form metric tables for longer sections until the full length of the code is reached (i.e., a procedure for combining metric tables). For each combination of two tables using the CombCPMT(x, y; z) procedure, construct the two-section trellis $T(\{x, y; z\})$ for the punctured code $p_{x,y}(C)$. Determine the number of real operations required to decode the code with the RMLD-(I,V) algorithm.

14.6 Decode the (16, 5) RM code with the RMLD-(I,V) algorithm using uniform sectionalization. At the beginning, the code is divided into eight sections, of 2 bits each. Devise a recursion procedure to combine composite path metric tables. For each combination of two adjacent metric tables, construct the special two-section trellis for the corresponding punctured code. Determine the total number of real operations required to decode the code.

14.7 Repeat Problem 14.6 by dividing the code into four sections, 4 bits per section, at the beginning of the recursion. Compare the computation complexity of this recursion with that of the recursion devised in Problem 14.6.

14.8 Devise an iterative decoding algorithm based on a minimum-weight trellis search using the ordered statistic decoding with order-1 reprocessing (presented in Section 10.8.30) to generate candidate codewords for optimality tests. Analyze the computational complexity of your algorithm. To reduce decoding computational complexity, the order i should be small, say $i = 0, 1$, or 2. The advantage of ordered statistic decoding over the Chase-II decoding is that it never fails to generate candidate codewords.

14.9 Simulate the error performance of the iterative decoding algorithm devised in Problem 14.8 for the (32, 16) RM code using order-1 reprocessing to generate 17 candidate codewords for testing and search of the ML codeword. Determine the average numbers of real operations and decoding iterations required for various SNR.

14.10 Decode the (32, 16) RM code with MAP and Max-log-Map decoding algorithms based on a uniform four-section trellis. Simulate and compare the error performances for two algorithms, and compare their computational complexities.

14.11 The (32, 16) RM code can be decomposed into eight parallel and structurally identical four-section subtrellises. Decode this code with the parallel Max-log-MAP algorithm. Compute the number of real operations required to process a single subtrellis and the total number of real operations required to decode the code. Also determine the size of the storage required to store the branch metrics, state metrics, and the likelihood ratios.

BIBLIOGRAPHY

1. A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," *IEEE Trans. Inform. Theory*, 13: 260–69, April 1967.

2. G. D. Forney, Jr., "The Viterbi Algorithm," *Proc. IEEE*, 61: 268–78, March 1973.

original form for the inner code decoding. This alternate permutation and inverse permutation is performed in each decoding iteration. Binary concatenation with this type of iterative decoding results in amazingly good error performance very close to the Shannon limit—of course, at the expense of decoding complexity and decoding delay.

The two-dimensional product codes without the checks on checks presented in Section 4.7 are quite suitable for the described type of iterative decoding. After the row (or column) encoding, the information bits of the information array are permuted pseudorandomly before the column (or row) encodings. This permutation allows the two sets of parity bits to provide two sets of uncorrelated estimates for the same set of information bits with iterative decoding. Row and column decodings are carried out alternately in an iterative manner.

The binary concatenation described here is in serial form; however, it can also be implemented in parallel form, in which the information sequence is encoded by two encoders independently using a pseudorandom interleaver. This encoding generates two independent sets of parity bits for the same information sequence. At the decoding side, iterative decoding is performed by two decoders based on these two sets of parity bits. Parallel concatenation is usually implemented using two convolutional encoders.

Binary concatenated coding schemes in parallel form using pseudorandom interleaving and iterative decoding, commonly called *turbo coding*, is the subject of Chapter 16.

PROBLEMS

15.1 Prove that the concatenation of an (n_1, k_1) inner code with minimum distance d_1 and an (n_2, k_2) outer code with minimum distance d_2 has a minimum distance of at least $d_1 d_2$.

15.2 Prove the lower bound of the minimum distance of an m-level concatenated code given by 15.12.

15.3 Consider the concatenation of a RS outer code over $GF(2^m)$ and the binary $(m+1, m, 2)$ single parity-check inner code. Devise an error-erasure decoding for this concatenated code. [*Hint:* During the inner code decoding, if parity failure is detected in $m+1$ received bits, an erasure is declared. If no parity failure is detected, the parity bit is removed to form a symbol in $GF(2^m)$].

15.4 Form a 5-level concatenated code with a minimum distance of 16 using RM codes of length 16 to form inner codes. Choose either binary or RS codes (or shortened RS codes) of length 16 as outer codes to maximize the overall code rate.

15.5 Decompose the $RM(2, 5)$ code into a 3-level concatenated code, and describe the trellis complexities of the component concatenated codes at the three levels.

15.6 Decompose the $RM(2, 6)$ code into a 3-level concatenated code, and give the trellis complexities of the component concatenated codes at the three levels.

15.7 Decode the $RM(2, 5)$ code with 3-stage decoding based on the decomposition obtained in Problem 17.5. Plot the bit- and block-error performances versus SNR.

15.8 Decode the $RM(2, 6)$ code with 3-stage decoding based on the decomposition obtained in Problem 17.6. Plot the bit- and block-error performances versus SNR.

15.9 Repeat Problem 17.7 with the IMS-MLD algorithm.

15.10 Repeat Problem 17.8 with the IMS-MLD algorithm.

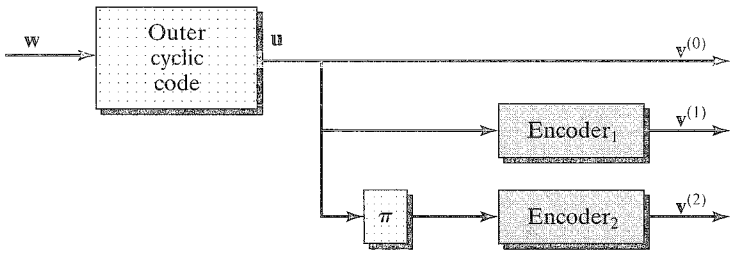


FIGURE 16.21: A concatenation of an outer cyclic code with an inner turbo code.

prematurely. For this reason it is usually advisable not to check the syndrome of the outer code during the first few iterations, when the probability of undetected error may be larger than the probability that the turbo decoder is error free. This method of stopping the iterations is particularly effective for large block lengths, since in this case the rate of the outer code can be made very high, thus resulting in a negligible overall rate loss.

For large block lengths, the foregoing idea can be extended to include outer codes, such as BCH codes, that can correct a small number of errors and still maintain a low undetected error probability. In this case, the iterations are stopped once the number of hard-decision errors at the output of the turbo decoder is within the error-correcting capability of the outer code. This method also provides a low word-error probability for the complete system; that is, the probability that the entire information block contains one or more decoding errors can be made very small. The idea of combining a turbo code with a high-rate outer BCH code was introduced in [45] and further analyzed in [46].

PROBLEMS

16.1 Prove that the general rate $R = 1/3$ turbo encoder shown in Figure 16.1(a), where encoders 1 and 2 are linear convolutional encoders (not necessary identical) separated by an arbitrary interleaver, is a linear system.

16.2 For the length $K = 16$ quadratic interleaver of (16.7), determine all pairs of indices that are interchanged by the permutation.

16.3 Consider a PCBC with two different constituent codes: the $(7, 4, 3)$ Hamming code and the $(8, 4, 4)$ extended Hamming code. Find the CWEFs, IRWEFs, and WEFs of this code assuming a uniform interleaver.

16.4 Find the IRWEFs and WEFs for Example 16.5.

16.5 Repeat Example 16.5 for the case $h = 4$. What is the minimum distance of the $(40, 16)$ PCBC if a 4×4 row–column (block) interleaver is used?

16.6 Consider a PCBC with the $(24, 12, 8)$ extended Golay code in systematic form as the constituent code.

a. Find the CWEFs $A_w(Z)$, $w = 1, 2, \cdots, 12$, of this code by generating the codewords of the $(23, 12, 7)$ Golay code in systematic form and then adding an overall parity check.

Assuming a uniform interleaver,

b. find the CWEFs $A_w^{PC}(Z)$, $w = 1, 2, \cdots, 12$;

c. find the IRWEFs $A^{PC}(W, Z)$ and $B^{PC}(W, Z)$; and

d. find the WEFs $A^{PC}(X)$ and $B^{PC}(X)$.

e. Now, consider a PCBC with the 12-repeated $(24, 12, 8)$ extended Golay code in systematic form as the constituent code. Assume that the information bits are arranged in a square array and that a row–column interleaver is used; that is, encoder 1 encodes across rows of the array, and encoder 2 encodes down columns of the array. Find the parameters (n, k, d) of the PCBC.

16.7 Prove (16.37).

16.8 Find the codeword IRWEF and WEF for the PCCC in Example 16.6.

16.9 Find the bit IRWEFs and WEFs for the PCCC in Example 16.6.

16.10 Repeat Example 16.6 for the encoder with the reversed generators given in (16.62).

16.11 Repeat Example 16.7 for the encoder with the reversed generators given in (16.62).

16.12 Find the multiplicity of weight-8 codewords in Example 16.8.

16.13 Repeat Example 16.8 using the feedforward encoder

$$\mathbb{G}_{ff}(D) = \begin{bmatrix} 1 & 1 + D + D^2 \end{bmatrix}$$

for the second constituent code.

16.14 Consider a rate $R = 1/4$ multiple turbo code (PCCC) with constituent encoder

$$\mathbb{G}(D) = [1 \quad (1 + D + D^2)/(1 + D)]$$

separated by two random interleavers (see Figure 16.2). Assuming a uniform interleaver and large block size K,

a. find the approximate CWEFs $A_w^{PC}(Z)$ and $B_w^{PC}(Z)$ for $w = 2, 3, 4, 5$;

b. find the approximate IRWEFs $A^{PC}(W, Z)$ and $B^{PC}(W, Z)$;

c. find the approximate WEFs $A^{PC}(X)$ and $B^{PC}(X)$; and

d. sketch the union bounds on $P_w(E)$ and $P_b(E)$ for $K = 1000$ and $K = 10000$, assuming a binary-input, unquantized-output AWGN channel.

16.15 Find the minimum-weight codewords corresponding to input weights 2 and 3 for the PCCCs whose generators are given in Table 16.6. In each case determine the free distance d_{free} assuming large K.

16.16 Show that for any $(n, 1, \nu)$ systematic feedforward encoder $A_w^{(w)}(Z) = \left[A_1^{(1)}(Z)\right]^w$ and that for any $(n, 1, \nu)$ systematic feedback encoder $A_{2w}^{(w)}(Z) = \left[A_2^{(1)}(Z)\right]^w$.

16.17 Show that a weight-1 input sequence cannot terminate an $(n, 1, \nu)$ systematic feedback encoder, but there always exists a weight-2 input sequence, of degree no greater than $2^\nu - 1$, that does terminate the encoder.

16.18 For an $(n, 1, \nu)$ systematic feedback encoder, show that the input sequence $\mathbf{u} = (1000\cdots)$ produces a cycle with input weight zero starting in state $S_1 = (10\cdots0)$, arriving in state $S_{2^\nu-1} = (0\cdots01)$ after at most $2^\nu - 2$ steps, and returning to state S_1 in one step.

16.19 For an $(n, 1, \nu)$ systematic feedback encoder, show that a 1 input from state $S_{2^\nu-1} = (0\cdots01)$ terminates the encoder.

16.20 Compute z_{min} and d_{eff} for the turbo codes with primitive and nonprimitive 16-state constituent codes D and E of Table 16.6.

16.21 Show that the bound of (16.97) is also valid for nonprimitive denominator polynomials.

16.22 Use the S-random interleaver algorithm to construct a length $K = 32$ permutation that breaks up all weight-2 input sequences with a spacing of $S = 4$ or less between 1's.

16.23 Prove that the Gaussian random variable $L_c r_l^{(0)}$ in (16.17) has variance $2L_c$ and mean $\pm L_c$.

16.24 Prove that for any real numbers w, x, and y, $\max^*(w+x, w+y) = w+\max^*(x, y)$.

16.25 Verify the α^* and β^* expressions in (16.114).

16.26 Verify all entries in Figure 16.19 that were not computed in the text.

16.27 Complete two more iterations of decoding in Examples 16.14 and 16.15. Is there any change in the decoded output?

16.28 Calculate the cross-entropy at the end of each complete iteration in Examples 16.14 and 16.15 and Problem 16.27.

16.29 [15] Consider the (8, 4, 3) PCBC formed by using $h = 2$ codewords from the (3, 2, 2) systematic single parity check (SPC) code, that is, a (6, 4, 2) 2-repeated SPC code, as the constituent code, along with a 2×2 block (row–column) interleaver of overall size $K = 4$. The information block is given by the vector $\mathbf{u} = [u_{11}, u_{12}, u_{21}, u_{22}]$, where u_{ij} represents the jth information bit in the ith row of the interleaver, $i, j = 1, 2$; the ith parity bit in the row code is given by $p_i^{(1)}, i = 1, 2$; and the jth parity bit in the column code is given by $p_j^{(2)}, j = 1, 2$. The arrangement is shown in Figure P-16.29(a). Assume the particular bit values given in Figure P-16.29(b) and the set of received channel L-values given in Figure P-16.29(c).

a. Use the trellis shown in Figure P-16.29(d) and the log-MAP algorithm to compute the extrinsic L-values for the first iteration of row and column decoding, and the soft-output L-values after the first complete iteration for each of the $K = 4$ information bits.

b. Repeat (a) using the Max-log-MAP algorithm.

16.30 Starting from (16.132), derive the cross-entropy expressions given in (16.133), (16.136), and (16.139).

u_{11}	u_{12}	$p_1^{(1)}$
u_{21}	u_{22}	$p_2^{(1)}$
$p_1^{(2)}$	$p_2^{(2)}$	

(8, 4, 3) PCBC

(a)

−1	−1	−1
−1	+1	+1
−1	+1	

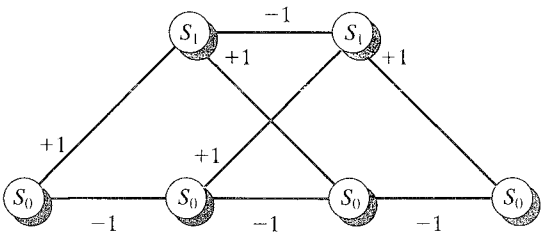
Coded values

(b)

−0.5	−1.5	−1.0
−4.0	−1.0	+1.5
−2.0	+2.5	

Received L-values

(c)



Decoding trellis

(d)

FIGURE P-16.29

significant improvement in error performance of a concatenated coding system with an RS code as the outer code is to be achieved, the RS outer code must be reasonably long and decoded with a sophisticated soft-decision decoding scheme that provides either optimal MLD performance or a suboptimal error performance. Unfortunately, the complexity of such a soft-decision decoding scheme or algorithm would be enormously large, and the decoder would be practically impossible to implement.

In this chapter we have shown that long high-rate finite-geometry LDPC codes with large minimum distances can be easily constructed and can be practically decoded with SPA decoding. They achieve very good error performance, especially the block-error performance. If such an LDPC code is used as the outer code in a concatenated coding system with a simple turbo code as the inner code, extremely good error performance and large coding gain should be achievable with practical implementation. With an LDPC code as the outer code and decoded with SPA decoding, the soft-output information provided by the inner turbo decoder can be fully utilized. We give an example to demonstrate the strength of such a combination of two powerful coding systems.

Consider a concatenated coding system in which the inner code is a high-rate block turbo code with the (64, 57) distance-4 Hamming code as the two constituent codes, and the outer code is the (65520, 61425) extended EG-LDPC code given in Example 17.14 [17]. The overall rate of this system is 0.75. The bit- and block-error performances of this concatenated LDPC-turbo coding system are shown in Figure 17.48. We see that this system achieves extremely good waterfall error performance. To achieve a BER of 10^{-6}, it requires an SNR of 2.35 dB, and at this BER, it performs only 0.7 dB away from the Shannon limit. This system is far superior to the concatenated coding scheme used in the NASA TDRS System presented in Section 15.6, whose overall rate is only 0.437.

Another form of concatenation of LDPC and turbo codes is to use an LDPC code as the two constituent codes in a parallel turbo coding arrangement, as described in Chapter 16. Because decoding of an LDPC code with the SPA is not trellis-based, a long LDPC code with large distance can be used as the constituent codes to achieve very good error performance without an error floor (or with an error floor at a very low error rate).

PROBLEMS

17.1 Does the following matrix satisfy the conditions of the parity-check matrix of an LDPC code given by Definition 17.1? Determine the rank of this matrix and give the codewords of its null space.

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

17.2 Form the transpose $\mathbf{H}^T$ of the parity-check matrix $\mathbf{H}$ given in Problem 17.1. Is $\mathbf{H}^T$ a low-density parity-check matrix? Determine the rank of $\mathbf{H}^T$ and construct the code given by the null space of $\mathbf{H}^T$.

17.3 Prove that the $(n, 1)$ repetition code is an LDPC code. Construct a low-density parity-check matrix for this code.

17.4 Consider the matrix $\mathbf{H}$ whose columns are all the m-tuples of weight 2. Does $\mathbf{H}$ satisfy the conditions of the parity-check matrix of an LDPC code? Determine the rank of $\mathbf{H}$ and its null space.

17.5 The following matrix is a low-density parity-check matrix. Determine the LDPC code given by the null space of this matrix. What is the minimum distance of this code?

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

17.6 Prove that the maximum-length code of length $2^m - 1$ presented in Section 8.3 is an LDPC code.

17.7 Construct the Tanner graph of the code given in Problem 17.1. Is the Tanner graph of this code acyclic? Justify your answer.

17.8 Construct the Tanner graph of the code given in Problem 17.2. Is the Tanner graph of this code acyclic? Justify your answer.

17.9 Construct the Tanner graph of the code given by the null space of the parity-check matrix given in Problem 17.5. Does the Tanner graph of this code contains cycles of length 6? Determine the number of cycles of length 6 in the graph.

17.10 Determine the orthogonal check-sums for every code bit of the LDPC code given by the null space of the parity-check matrix of Problem 17.5.

17.11 Prove that the minimum distance of the Gallager-LDPC code given in Example 17.2 is 6.

17.12 Determine the generator polynomial of the two-dimensional type-I $(0, 3)$th-order cyclic EG-LDPC code constructed based on the two-dimensional Euclidean geometry $\mathrm{EG}(2, 2^3)$.

17.13 Determine the parameters of the parity-check matrix of the three-dimensional type-I (0,2)th-order cyclic EG-LDPC code $C_{EG,c}^{(1)}(3, 0, 2)$. Determine the generator polynomial of this code. What are the parameters of this code?

17.14 Determine the parameters of the companion code of the EG-LDPC code given in Problem 17.13.

17.15 Decode the two-dimensional type-I $(0, 3)$th-order cyclic EG-LDPC code with one-step majority-logic decoding and give the bit- and block-error performance for the AWGN channel with BPSK signaling.

17.16 Repeat Problem 17.15 with BF decoding.

17.17 Repeat Problem 17.15 with weighted majority-logic decoding.

17.18 Repeat Problem 17.15 with weighted BF decoding.

17.19 Repeat Problem 17.15 with SPA decoding.

17.20 Decode the three-dimensional type-II $(0, 2)$th-order quasi-cyclic EG-LDPC code given in Problem 17.14 with SPA decoding, and give the bit- and block-error performance of the code for the AWGN channel with BPSK signaling.

17.21 Consider the parity-check matrix $\mathbf{H}_{EG,c}^{(1)}$ of the three-dimensional type-I $(0, 2)$th-order cyclic EG-LDPC code given in Problem 17.13. Split each column of this

parity-check matrix into five columns with rotating weight distribution. The result is a new low-density parity-check matrix that gives an extended EG-LDPC code. Decode this code with SPA decoding and give its bit- and block-error performances.

17.22 Construct a parity-check matrix of the Gallager-LDPC code with the following parameters: $m = 6$, $\rho = 4$, and $\gamma = 3$. Choose column permutations for the submatrices such that λ is no greater than 1.

17.23 Prove that the Tanner graph of a finite-geometry LDPC code contains cycles of length 6. Enumerate the number of cycles of length 6.

17.24 Prove that the minimum distance of an EG-Gallager LDPC code must be even. Use the result to prove the lower bound on minimum distance given by (17.68).

17.25 Construct an EG-Gallager LDPC code using six parallel bundles of lines in the two-dimensional Euclidean geometry EG(2,2^5) over $GF(2^5)$. Compute its bit- and block-error performances with SPA decoding.

17.26 Construct a masked EG-Gallager LDPC code of length 1024 by decomposing the incidence matrices of eight parallel bundles of lines in EG(2, 2^5) into 32×32 permutation matrices. To construct such a code, set $\rho = 32$, and form an 8×32 masking matrix with column and row weights 4 and 16, respectively, using four primitive 8-tuples over $GF(2)$. Compute the bit- and block-error performances using SPA decoding.

17.27 The incidence vectors of the lines in EG(2, 2^5) not passing through the origin form a single 1023×1023 circulant G with weight 32. Construct a rate-1/2 quasi-cyclic code of length 8184 by decomposing G into a 4×8 array of 1023×1023 circulant permutation matrices. Compute the bit- and block-error performance of the code with SPA decoding.

17.28 Prove that there exist a primitive element α in $GF(241)$ and an odd positive integer c less than 241 such that $\alpha^{64} + 1 = \alpha^c$.

17.29 Design a concatenated turbo coding system with a finite-geometry LDPC code of your choice as the outer code. Construct the inner turbo code by using the second-order (32, 16) RM code as the component code. Give the bit-error performance of your designed system.

BIBLIOGRAPHY

1. R. G. Gallager, "Low Density Parity Check Codes," *IRE Trans. Inform. Theory*, IT-8: 21–28, January 1962.

2. R. G. Gallager, *Low Density Parity Check Codes*, MIT Press, Cambridge, 1963.

3. R. M. Tanner, "A Recursive Approach to Low Complexity Codes," *IEEE Trans. Inform. Theory*, IT-27: 533–47, September 1981.

4. D. J. C. MacKay and R. M. Neal, "Near Shannon Limit Performance of Low Density Parity Check Codes," *Electron. Lett.*, 32 (18): 1645–46, 1996.

5. M. Sipser and D. Spielman, "Expander Codes," *IEEE Trans. Inform. Theory*, 42 (6): 1710–22, November 1996.

6. D. Spielman, "Linear-Time Encodable Error-Correcting Codes," *IEEE Trans. Inform. Theory*, 42 (6): 1723–31, November 1996.

7. M. C. Davey and D. J. C. MacKay, "Low Density Parity Check Codes over $GF(q)$," *IEEE Commun. Lett.*, 2(6), 165–67, June 1998.

V.29 modem standard was adopted in 1976 little progress was made in increasing the speed and quality of data transmission over voice-grade telephone lines until the appearance of the V.32 and V.33 standards in 1986 (see Example 18.14). The V.29 standard used uncoded 16-QAM and a 2400 symbols/second signaling rate to achieve a spectral efficiency of $\eta = 4.0$ bits/symbol and a transmission speed of 9600 bps in a half-duplex (one-way) mode. Owing to the bandwidth constraints of the channel, signaling rates higher than 2400 symbols/second were not considered feasible. Thus, the only avenue to increased data rates was to expand the size of the signal constellation; however, because of the SNR constraints of the channel, this meant that signals had to be packed closer together, resulting in degraded performance. Thus, a clear need developed for a scheme that could allow constellation expansion at the same signaling rate, thus achieving higher data rates, and yet provide a coding gain to at least recover the noise margin lost by the closer packing of signals. TCM proved to be just such a scheme and, combined with some sophisticated signal-processing techniques, has resulted in a series of improvements that have pushed modem speeds to 56 Kbps.

PROBLEMS

18.1 Prove equation (18.8).

18.2 Find, as functions of the parameter d, the AEWEs $\Delta_{\mathbf{e}}^2(X)$ and the MEWEs $\delta_{\mathbf{e}}^2(X)$ for the two signal set mappings shown in Figure P-18.2, and determine if they are uniform. Assume each constellation has unit average energy.

18.3 Determine if an isometry exists between the subsets $Q(0)$ and $Q(1)$ for the two signal set mappings in Problem 18.2.

18.4 Use Lemma 18.1 to prove that for uniform mappings, $A_{av}(X)$ can be computed by labeling the error trellis with the AEWEs and finding the transfer function of the modified state diagram.

18.5 Construct a counterexample to show that Lemma 18.1 does not necessarily hold for rate $R = k/(k+2)$ codes. State a rate $R = k/(k+2)$ code lemma, similar to Lemma 18.1, specify the conditions for uniformity, and prove the lemma.

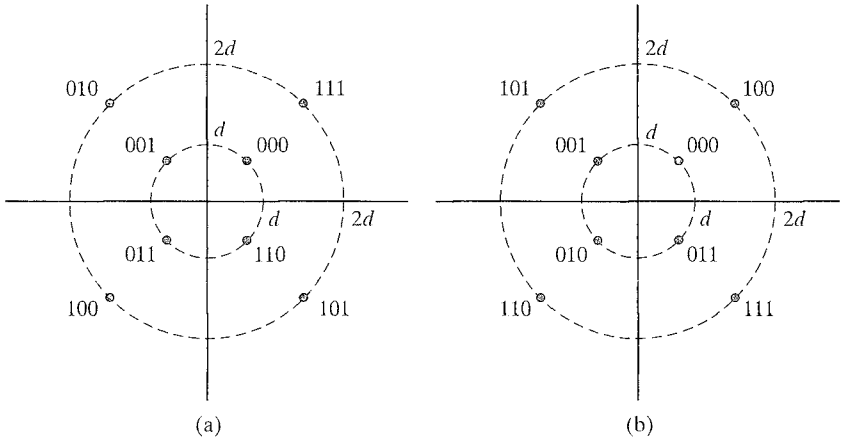


FIGURE P-18.2

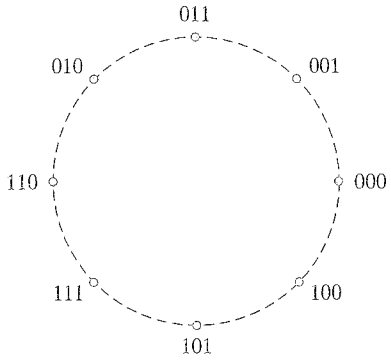


FIGURE P-18.8

18.6 Determine the AEWEs $\Delta_e^2(X)$ and the MEWEs $\delta_e^2(X)$ for Gray- and naturally mapped 4-AM and show that they are both uniform mappings.

18.7 Consider mapping a rate $R = 2/3$ convolutional code into 8-AM using natural mapping.

a. Determine the AEWEs $\Delta_e^2(X)$ and the MEWEs $\delta_e^2(X)$ for this mapping.

b. Determine if the mapping is uniform.

c. Find the coding gain (or loss) γ for the three 4-state, rate $R = 2/3$ convolutional codes of Example 18.4 compared with uncoded QPSK.

d. Can you find a 4-state, rate $R = 2/3$ convolutional code with a better coding gain when used with naturally mapped 8-AM?

18.8 Show that the Gray mapping of the 8-PSK signal set shown in Figure P-18.8 is not uniform.

18.9 Repeat Example 18.4, finding the MFSE distances and asymptotic coding gains for three rate $R = 2/3$ trellis-coded 8-PSK systems, if natural mapping is replaced by the uniform mapping of Figure 18.2(a). Compare the results with natural mapping.

18.10 Repeat Example 18.5 by finding a counterexample to the rate $R = k/(k+1)$ code lemma for the nonuniform signal set mapping in Problem 18.2(a).

18.11 Repeat Example 18.4, finding the MFSE distances and asymptotic coding gains for three rate $R = 2/3$ trellis-coded 8-PSK systems, if natural mapping is replaced by the nonuniform Gray-mapped 8-PSK signal set in Problem 18.8. (In this case, since the rate $R = k/(k+1)$ code lemma is not satisfied, the distances between all possible path pairs must be considered.) Compare the results with natural mapping.

18.12 Show that set partitioning of the infinite two-dimensional integer lattice $\mathbb{Z}^2$ results in a regular mapping.

18.13 Apply mapping by set partitioning to the 32-CROSS signal constellation and determine the error vectors $\mathbf{e}$ for which (18.26) is not satisfied with equality.

18.14 Construct an example in which (18.25) and (18.27) do not give the same result.

18.15 Apply mapping by set partitioning to the 8-AM signal constellation and determine the MSSDs Δ_i^2, $i = 0, 1, 2$. Find the asymptotic coding gain γ and the average number of nearest neighbors $A_{d_{free}}$ when the 4-state code of Table 18.6(a) is applied to 8-AM. Repeat for the one-dimensional integer lattice $\mathbb{Z}^1$.

18.16 Compute, as functions of the parameter d, the asymptotic coding gains of the 16-QAM codes in Table 18.6(b) compared with the following uncoded constellations:

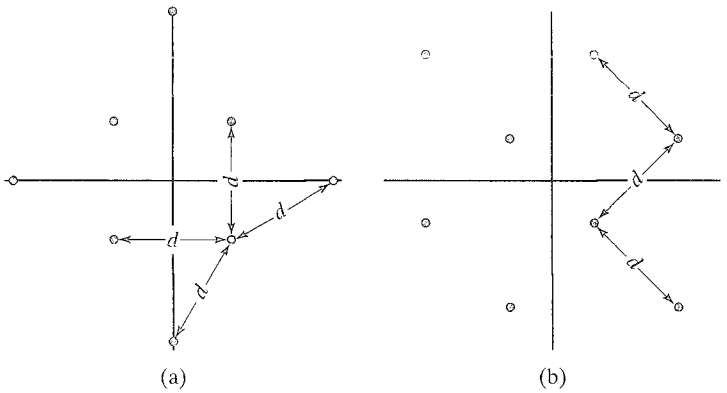


FIGURE P-18.16

(i) the 8-CROSS constellation shown in Figure P-18.16(a) and (ii) the 8-QAM constellation shown in Figure P-18.16(b). Assume each constellation has unit average energy.

18.17 Calculate $A_{av}^{t}(W, X)$ for Example 18.9.

18.18 Apply mapping by set partitioning to the 8-QAM signal constellation shown in Problem 18.16 and determine the MSSDs $\Delta_i^2, i = 0, 1, 2$. Find $A_{av}^{t}(W, X)$ and $A_{av}^{p}(W, X)$ for the code of Example 18.9 using this constellation.

18.19 Let $\mathbb{1}(D) = 1 + D + D^2 + D^3 + \cdots$ in Example 18.10 and recalculate (18.37) and (18.40). Are the conditions for rotational invariance affected?

18.20 Derive general conditions on the number of terms in $\mathbb{h}^{(1)}(D)$ and $\mathbb{h}^{(0)}(D)$ to satisfy (18.46).

18.21 Show that (18.52) is still satisfied when the rotated binary sequences for naturally mapped QPSK given in (18.38) are substituted into the equation, and $\mathbb{h}^{(0)}(D)$ has an odd number of nonzero terms.

18.22 Verify that (18.52) is satisfied for the encoder of (18.53) when the rotated binary sequences for naturally mapped QPSK given in (18.38) are substituted into the equation.

18.23 Find minimal encoder realizations for the 90° rotationally invariant $\nu = 4$ and $\nu = 5$ nonlinear rate $R = 1/2$ codes based on the parity-check matrices

$$\mathbb{H}(D) = [(D^3 + D)/(D^4 + D + 1) \quad 1]$$

and

$$\mathbb{H}(D) = [(D^4 + D)/(D^5 + D^2 + 1) \quad 1],$$

respectively. Show that the $\nu = 5$ case cannot be realized with 32 states.

18.24 Derive general conditions on the number of nonzero terms in $\mathbb{h}^{(2)}(D)$, $\mathbb{h}^{(1)}(D)$, and $\mathbb{h}^{(0)}(D)$ to satisfy (18.59).

18.25 Show that the 45° rotated binary code sequences for naturally mapped 8-PSK are given by $\mathbb{v}_r^{(2)}(D) = \mathbb{v}^{(2)}(D) \oplus \mathbb{v}^{(1)}(D) \circ \mathbb{v}^{(0)}(D)$, $\mathbb{v}_r^{(1)}(D) = \mathbb{v}^{(1)}(D) \oplus \mathbb{v}^{(0)}(D)$, and $\mathbb{v}_r^{(0)}(D) = \mathbb{v}^{(0)}(D) \oplus \mathbb{1}(D)$.

18.26 Show that (18.61) is still satisfied when the rotated binary sequences for naturally mapped 8-PSK given in Problem 18.25 are substituted into the equation, and $\mathbb{h}^{(0)}(D)$ has an odd number of nonzero terms.

18.27 Show how $f(D)$ in (18.65b) can be rewritten to correspond to the encoder realization shown in Figure 18.25.

18.28 Use the method of Euclidean weights to show that $d^2_{free} = 3.515$ for 16-state, rate $R = 2/3$, trellis-coded 8-PSK with $\mathbb{h}^{(2)} = (1\ 6)$, $\mathbb{h}^{(1)} = (1\ 2)$, and $\mathbb{h}^{(0)} = (2\ 3)$.

18.29 Prove (18.88); that is, the partition level p equals the sum of the redundancies of the I linear block codes that define the subcode $\Lambda_p(0)$.

18.30 Draw the appropriate signal set mappers, similar to Figure 18.30, for the three 3 × 8-PSK partitions of Example 18.17.

18.31 Draw the complete encoder diagram for the 8-state, 2×16-PSK, $\eta = 3.5$ bits/symbol encoder listed in Table 18.15(b), including differential encoding of appropriate input bits. Use (18.93) to express the first three 2×16-PSK encoder output signals in both binary and integer form, assuming the input sequence $\mathbb{u} = (\mathbb{u}_0, \mathbb{u}_1, \mathbb{u}_2, \cdots) = (1011001, 0001110, 1101110, \cdots)$, and the encoder starts in the all-zero state.

18.32 Use the approach of Example 18.19 to determine the rotational invariance of the two 16-state, 3×8-PSK, $\eta = 2.33$ bits/symbol encoders listed in Table 18.15(a).

18.33 Draw the augmented, modified state diagram and find the AIOWEFs in Example 18.20. Include sketches of $P_b(E)$ versus E_s/N_0 and uncoded QPSK, and estimate the real coding gain at a BER of 10^{-5}.

18.34 Repeat Example 18.20 for (1) a 2×16-QAM system with $\eta = 3.5$ bits/symbol and (2) trellis-coded $\mathbb{Z}^4$, using the 8-state code listed in Table 18.15(c) with $q = 0$.

18.35 Assuming a distance of d between neighboring signal points, calculate the average energies of the 192-point signal set in Figure 18.34 and of its shaped 4-D version as functions of d, and compute the shaping gain.

18.36 Assuming a distance of d between neighboring signal points, compute the CERs (compared with 2-AM) and the PARs of the 1-D signal sets 2-AM, 4-AM, and 8-AM as functions of d.

18.37 Draw the encoder corresponding to the rate $R = 2/3$ parity-check matrix of (18.112), and show that it is equivalent to the encoder in Figure 18.35.

BIBLIOGRAPHY

1. G. Ungerboeck, "Channel Coding with Multilevel/Phase Signals," *IEEE Trans. Inform. Theory*, IT-28: 55–67, January 1982.

2. G. Ungerboeck and I. Csajka, "On Improving Data-Link Performance by Increasing the Channel Alphabet and Introducing Sequence Coding," in *IEEE Int. Symp. Inform. Theory (ISIT 1976) Book of Abstracts*, p. 53, Ronneby, Sweden, June 1976.

3. G. Ungerboeck, "Trellis-Coded Modulation with Redundant Signal Sets. Part I: Introduction," *IEEE Commun. Mag.*, 25: 5–11, February 1987.

4. _____, "Trellis-Coded Modulation with Redundant Signal Sets. Part II: State of the Art," *IEEE Commun. Mag.*, 25: 12–21, February 1987.

5. J. L. Massey, "Coding and Modulation in Digital Communications," in *Proc. 1974 Zurich Seminar on Digital Communications*, pp. E2(1)–E2(4), Zurich, Switzerland, March 1974.

6. J. B. Anderson and D. P. Taylor, "A Bandwidth-Efficient Class of Signal Space Codes," *IEEE Trans. Inform. Theory*, IT-24: 703–12, November 1978.

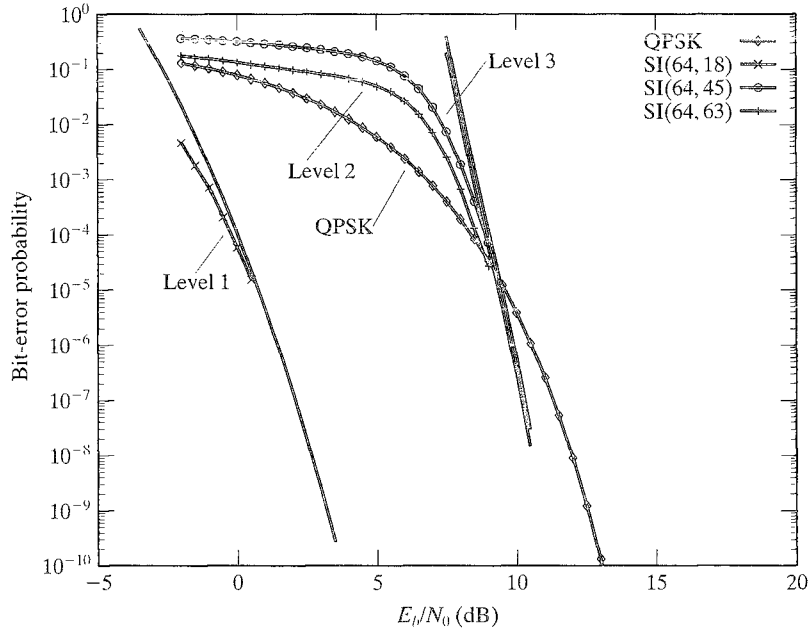


FIGURE 19.29: Bit-error performance of various levels of a 3-level 8-PSK BCM code for unequal error protection with hybrid signal set partition.

PROBLEMS

19.1 Prove that the minimum squared Euclidean distance of the 3-level 8-PSK code given in Example 19.1 is equal to 4.

19.2 Construct a 3-level 8-PSK code with the following three binary component codes: (1) C_1 is the (16, 1, 16) repetition code; (2) C_2 is the (16, 11, 4) second-order RM code; and (3) C_3 is the (16, 15, 2) single parity code.

- **a.** Determine the spectral efficiency of the code.
- **b.** Determine the minimum squared Euclidean, symbol, and product distances of the code.
- **c.** Analyze the trellis complexity of the code.

19.3 Decode the 3-level 8-PSK code constructed in Problem 19.2 with a single-stage Viterbi decoding, and compute its error performance for an AWGN channel.

19.4 Replace the first component code C_1 in Problem 19.2 with the first-order (16, 5, 8) RM code. Construct a new 3-level 8-PSK code. Determine its spectral efficiency, minimum squared Euclidean, symbol, and product distances. Analyze its trellis complexity.

19.5 Decode the code constructed in Problem 19.4 with a three-stage soft-decision decoding. Each component code is decoded with Viterbi decoding based on its trellis. Compute its error performance for an AWGN channel.

19.6 Design a single-level concatenated coded modulation system with the NASA standard (255, 223) RS code over $GF(2^8)$ as the outer code and a 3-level 8-PSK code of length 16 as the inner code. The inner code is constructed using the following binary codes as the component codes: (1) C_1 is the (16, 1, 16) repetition code; (2) C_2 is the (16, 15, 2) single-parity-check code; and (3) C_2 is the (16, 16, 1)

universal code. What is the spectral efficiency of the overall system? Decode the inner code with a single-stage Viterbi decoding and the outer code with an algebraic decoding. Compute the error performance of the system for an AWGN channel.

BIBLIOGRAPHY

1. H. Imai and S. Hirakawa, "A New Multilevel Coding Method Using Error-Correcting Codes," *IEEE Trans. Inform. Theory*, 23 (3): 371–76, May 1977.

2. V. V. Ginzburg, "Multidimensional Signals for a Continuous Channel," *Probl. Peredachi Inform.*, 20 (1): 28–46, 1984.

3. S. I. Sayegh, "A Class of Optimum Block Codes in Signal Spaces," *IEEE Trans. Commun.*, 30 (10): 1043–45, October 1986.

4. R. M. Tanner, "Algebraic Construction of Large Euclidean Distance Combined Coding Modulation Systems," *Abstracts of Papers, IEEE Int. Symp. Inform. Theory*, Ann Arbor, Mich., October 6–9, 1986.

5. G. J. Pottie and D. P. Taylor, "Multilevel Channel Codes Based on Partitioning," *IEEE Trans. Inform. Theory*, 35 (1): 87–98, January 1989

6. A. R. Calderbank, "Multilevel Codes and Multistage Decoding," *IEEE Trans. Commun.*, 37 (3): 222–29, March 1989.

7. T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On Linear Structure and Phase Rotation Invariant Properties of Block 2^l-PSK Modulation Codes," *IEEE Trans. Inform. Theory*, 37 (1): 164–67, January 1991.

8. T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On Multilevel Block Modulation Codes," *IEEE Trans. Inform. Theory*, 37 (4): 965–75, July 1991.

9. J. Wu and S. Lin, "Multilevel Trellis MPSK Modulation Codes for the Rayleigh Fading Channels," *IEEE Trans. Commun.*, 41 (9): 1311–18, September 1993.

10. G. D. Forney, Jr., "Coset Codes II: Binary Lattices and Related Codes," *IEEE Trans. Inform. Theory*, 34 (5): 1152–87, September 1988.

11. T. Takata, S. Ujita, T. Kasami, and S. Lin, "Multistage Decoding of Multilevel Block MPSK Modulation Codes and Its Performance Analysis," *IEEE Trans. Inform. Theory*, 39 (4): 1204–18, July 1993.

12. T. Woerz and J. Hagenauer, "Multistage Coding and Decoding for a MPSK System," *Proc. IEEE Global Telecommun. Conf.*, pp. 698–703, San Diego, Calif., December 1990.

13. T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "A Concatenated Coded Modulation Scheme for Error Control," *IEEE Trans. Commun.*, 38 (6): 752–63, June 1990.

By combining Fire codes and BCH codes and with the aid of a computer, Hsu et al. have constructed several classes of shortened cyclic codes that are capable of correcting burst errors as well as random errors [26]. Other works on constructing burst-and-random error-correcting block codes can be found in [11, 19, and 26–28].

PROBLEMS

20.1 Show that if an (n, k) cyclic code is designed to correct all burst errors of length l or less and simultaneously to detect all burst errors of length $d \geq l$ or less, the number of parity-check digits of the code must be at least $l + d$.

20.2 Devise an error-trapping decoder for an l-burst-error-correcting cyclic code. The received polynomial is shifted into the syndrome register from the right end. Describe the decoding operation of your decoder.

20.3 Prove that the Fire code generated by (20.4) is capable of correcting any error burst of length l or less.

20.4 The polynomial $\mathfrak{p}(X) = 1 + X + X^4$ is a primitive polynomial over $GF(2)$. Find the generator polynomial of a Fire code that is capable of correcting any single error burst of length 4 or less. What is the length of this code? Devise a simple error-trapping decoder for this code.

20.5 Devise a high-speed error-trapping decoder for the Fire code constructed in Problem 20.4. Describe the decoding operation.

20.6 Use a code from Table 20.3 to derive a new code with burst-error-correcting capability $l = 51$, length $n = 255$, and burst-error-correcting efficiency $z = 1$. Construct a decoder for this new code.

20.7 Let $\mathfrak{g}(X)$ be the generator polynomial of an (n, k) cyclic code. Interleave this code to degree λ. The resultant code is a $(\lambda n, \lambda k)$ linear code. Show that this interleaved code is cyclic and its generator polynomial is $\mathfrak{g}(X^{\lambda})$.

20.8 Show that the Burton code generated by $\mathfrak{g}(X) = (X^m + 1)\mathfrak{p}(X)$, where $\mathfrak{p}(X)$ is an irreducible polynomial of degree m, is capable of correcting all phased bursts confined to a single subblock of m digits.

20.9 Let $m = 5$. Construct a Burton code that is capable of correcting any phased burst confined to a single subblock of five digits. Suppose that this code is interleaved to degree $\lambda = 6$. What are the length, the number of parity-check digits, and the burst-error-correcting capability of this interleaved code?

20.10 Interleave the (164, 153) code in Table 20.3 to degree $\lambda = 6$. Compare this interleaved code with the interleaved Burton code of Problem 20.9. Which code is more efficient?

20.11 Interleave the (15, 7) BCH code to degree 7. Discuss the error-correcting capability of this interleaved code. Devise a decoder for this code and describe the decoding operation.

20.12 Consider the (31, 15) RS code with symbols from $GF(2^5)$. Convert this RS code to a binary code. Discuss the error-correcting capability of the binary RS code.

20.13 Suppose that the Fire code constructed in Problem 20.4 is shortened by deleting the 15 high-order message digits. Devise a decoder for the shortened code such that the 15 extra shifts of the syndrome register after the received vector has entered can be avoided.

20.14 Find a modified Fire code of length 63 that is capable of correcting any single burst of length 4 or less as well as any combination of two or fewer random errors. Determine its generator polynomial.

20.15 Consider the modified Fire code C generated by $\mathfrak{g}(X)$ of (20.9). Show that a burst of length $(b + 1)/2$ or less and error pattern of weight t or less cannot be in the same coset.

PROBLEMS

21.1 Using mathematical induction, show that the unknown elements of the matrix $\mathbb{B}_0$ can always be chosen so that (21.11) is satisfied.

21.2 Show how to construct optimum phased-burst-error-correcting Berlekamp–Preparata codes with $k < n - 1$.

21.3 Consider the Berlekamp–Preparata code with $n = 3$.
- a. Find m, b, and g for this code.
- b. Find the $\mathbb{B}_0$ matrix.
- c. Find the generator polynomials $\mathbb{g}_1^{(2)}(D)$ and $\mathbb{g}_2^{(2)}(D)$.
- d. Find the $\mathbb{H}_0$ matrix.
- e. Draw the complete encoder/decoder block diagram for this code.

21.4 Consider the Iwadare–Massey code with $n = 2$ and $\lambda = 4$.
- a. Find m, b, and g for this code.
- b. Find the generator polynomial $\mathbb{g}^{(1)}(D)$.
- c. Find the repeat distance of the information error bit $e_l^{(0)}$.
- d. Draw the complete encoder/decoder block diagram for this code.

21.5 A second class of Iwadare–Massey codes exists with the following parameters:

$$m = (2n - 1)\lambda + (n^2 - n - 2)/2$$

$$b = n\lambda$$

$$g = n(m + 1) - 1$$

The $n - 1$ generator polynomials are given by (21.20), where $a(i) \triangleq \frac{1}{2}(n - i)(4\lambda + n - i - 3) + n - 1$, and $b(i) \triangleq \frac{1}{2}(n - i)(4\lambda + n - i - 1) + n + \lambda - 2$. Consider the code with $n = 3$ and $\lambda = 3$.
- a. Find m, b, and g for this code.
- b. Find the generator polynomials $\mathbb{g}_1^{(2)}(D)$ and $\mathbb{g}_2^{(2)}(D)$.
- c. Find the repeat distance of the information error bits $e_l^{(0)}$ and $e_l^{(1)}$.
- d. Construct a decoding circuit for this code.

21.6 Construct a general decoding circuit for the class of Iwadare–Massey codes in Problem 21.5. For the two classes of Iwadare–Massey codes:
- a. compare the excess guard space required beyond the Gallager bound; and
- b. compare the number of register stages required to implement a general decoder.

21.7 Show that for the Iwadare–Massey code of Example 21.4, if $n[m+(\lambda+2)n-1]-1 = 95$ consecutive error-free bits follow a decoding error, the syndrome will return to the all-zero state.

21.8 Consider the $(2, 1, 5)$ double-error-correcting orthogonalizable code from Table 13.3 interleaved to degree $\lambda = 7$.
- a. Completely characterize the multiple-burst-error-correcting capability and the associated guard-space requirements of this interleaved code.
- b. Find the maximum single-burst length that can be corrected and the associated guard space.
- c. Find the ratio of guard space to burst length for (b).
- d. Find the total memory required in the interleaved decoder.
- e. Draw a block diagram of the complete interleaved system.

21.9 Consider the interleaved encoder shown in Figure 21.6(b). Assume that an information sequence $u_0, u_1, u_2, \cdots$ enters the encoder. Write down the string of encoded bits and verify that an interleaving degree of $\lambda = 5$ is achieved.

21.10 Consider the Berlekamp–Preparata code of Problem 21.3 interleaved to degree $\lambda = 7$.
- a. Find the g/b ratio and compare it with the Gallager bound.
- b. Draw a block diagram of the complete interleaved system.

21.11 Consider the $n = 3$ Berlekamp–Preparata code interleaved to degree $\lambda = 7$ and the $n = 3$ Iwadare–Massey code with $\lambda = 7$.
- a. Compare the g/b ratios of the two codes.
- b. Compare the number of register stages required to implement the decoder in both cases.

21.12 Consider the (2, 1, 9) systematic code with $\mathbf{g}^{(1)}(D) = 1 + D^2 + D^5 + D^9$.
- a. Is this code self-orthogonal? What is t_{ML} for this code?
- b. Is this a diffuse code? What is the burst-error-correcting capability b and the required guard space g?
- c. Draw a complete encoder/decoder block diagram for this code.

21.13 For the diffuse code of Figure 21.7, find the minimum number of error-free bits that must be received following a decoding error to guarantee that the syndrome returns to the all-zero state.

21.14 Consider using the (2, 1, 11) triple-error-correcting orthogonalizable code from Table 13.3 in the Gallager burst-finding system.
- a. Draw a block diagram of the encoder.
- b. Draw a block diagram of the decoder.
- c. With $t'_{ML} = 1$, choose M and L such that the probabilities of an undetected burst and of a false return to the r-mode are less than 10^{-2} and the g/b ratio is within 1% of the bound on "almost all" burst-error correction for rate $R = 1/2$ codes.
- d. Repeat (c) for $t'_{ML} = 2$.

21.15 Consider the rate $R = 2/3$ burst-trapping code of Example 21.8.
- a. Choose L such that the g/b ratio is within 1% of the bound on "almost all" burst-error correction for rate $R = 2/3$ codes.
- b. Describe the generator matrix $\mathbf{G}$ of the (30, 20, 2L) convolutional code.

BIBLIOGRAPHY

1. D. W. Hagelbarger, "Recurrent Codes: Easily Mechanized Burst-Correcting, Binary Codes," *Bell System Tech. J.*, 38: 969–84, July 1959.

2. Y. Iwadare, "On Type B1 Burst-Error-Correcting Convolutional Codes," *IEEE Trans. Inform. Theory*, IT-14: 577–83, July 1968.

3. R. G. Gallager, *Information Theory and Reliable Communication*. McGraw-Hill, New York, 1968.

4. A. D. Wyner and R. B. Ash, "Analysis of Recurrent Codes," *IEEE Trans. Inform. Theory*, IT-9: 143–56, July 1963.

5. E. R. Berlekamp, "Note on Recurrent Codes," *IEEE Trans. Inform. Theory*, IT-10: 257–58, July 1964.

6. F. P. Preparata, "Systematic Construction of Optimal Linear Recurrent Codes for Burst Error Correction," *Calcolo*, 2: 1–7, 1964.

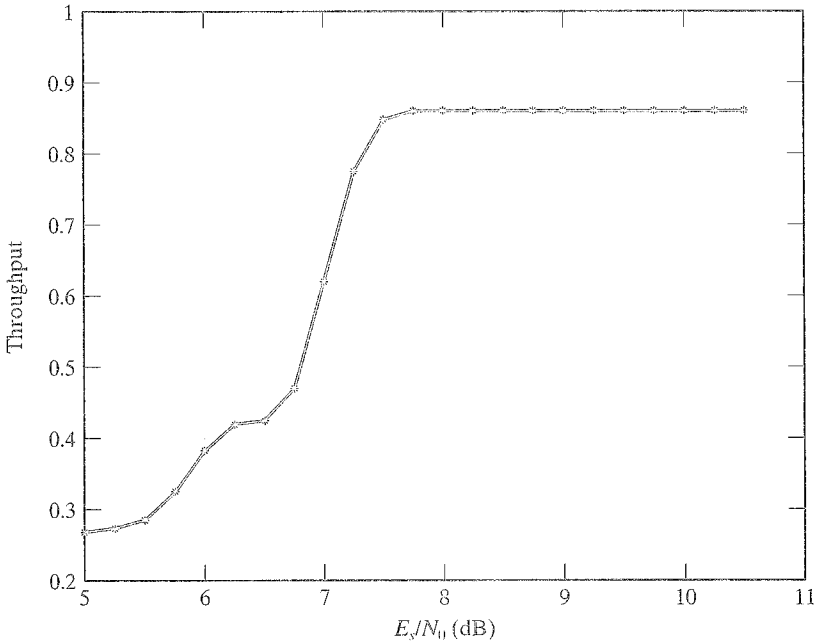


FIGURE 22.26: Lower bound on the throughput efficiency.

the concatenated code is $R = R_1 \times R_2 = 1 \times 192/224 = 0.857$ (or spectral efficiency of 1.714 bits/signal).

The half-rate invertible code C_r for parity retransmission is the shortened (64, 32) RS code over $GF(2^8)$ obtained from shortening the outer code C_2. C_r is capable of correcting up to 16 symbol errors over a span of 64 symbols and hence is very powerful. Therefore, even in a very noisy situation, a transmitted data array should be recovered with at most one retransmission.

The reliability and throughput efficiency of this system have been analyzed in [51] and are shown in Figures 22.25 and 22.26, respectively. The system performs extremely well for SNR E_s/N_0 greater than 7 dB (or, equivalently, channel bit-error probability $p \leq 10^{-2}$). For SNR $E_s/N_0 = 8$ dB, error-free communication is practically achieved and the system throughput efficiency is equal to the system rate, 0.857.

Other hybrid ARQ schemes using coded modulation for error control can be found in [51, 53, and 64–66].

PROBLEMS

22.1 In (22.5) we saw that the throughput of the go-back-N ARQ depends on the channel block error rate $P = 1 - (1 - p)^n$, where n is the code block length, and p is the channel (BSC) transition probability. Let τ be the data rate in bits per second. Let T be the round-trip delay time in seconds. Then, $N = \tau \cdot T/n$. Suppose that p and k/n are fixed. Determine the block length n_0 that maximizes the throughput η_{GBN}. The block length n_0 is called the *optimal block length*.

Optimal block lengths for the three basic ARQ schemes were investigated by Morris [7].

22.2 Consider a continuous ARQ scheme that operates as follows. When the transmitter receives a NAK for a particular vector $\mathbf{v}$ under the condition that the $N-1$ vectors preceding $\mathbf{v}$ have been positively acknowledged, the transmitter stops sending new vectors and simply repeats the vector $\mathbf{v}$ continuously until an ACK for $\mathbf{v}$ is received. After receiving an ACK, the transmitter renews transmission of new vectors. At the receiver, when a received vector $\tilde{\mathbf{v}}$ is detected in error under the condition that all the vectors preceding $\tilde{\mathbf{v}}$ have been successfully received, the receiver rejects $\tilde{\mathbf{v}}$ and all the $N-1$ subsequent received vectors until the first repetition of $\mathbf{v}$ arrives. Then, the receiver checks the syndrome of $\tilde{\mathbf{v}}$ and the following repetitions of $\mathbf{v}$. An ACK is sent to the transmitter as soon as one repetition of $\mathbf{v}$ has been successfully received.

a. Derive the throughput of this scheme.

b. Compare the throughput of this scheme and the throughput of the conventional go-back-N ARQ.

22.3 Suppose that we use the retransmission strategy described in Problem 22.2 but with a buffer of size N provided at the receiver. When a received vector $\tilde{\mathbf{v}}$ is detected in error, the receiver stores the subsequent successfully received vectors. When a repetition of $\mathbf{v}$ is successfully received, the receiver releases $\tilde{\mathbf{v}}$ and the error-free vectors held in the receiver buffer in consecutive order until the next erroneous vector is encountered.

a. Derive the throughput of this ARQ scheme.

b. Compare its throughput with that of the conventional go-back-N ARQ.

22.4 We may shorten the (31, 16) BCH code to obtain a (30, 15) invertible code. Devise an inversion circuit for this code.

22.5 In a stop-and-wait ARQ system, suppose that the forward channel is a BSC with transition probability p_1, and the feedback channel is a BSC with transition probability p_2. Derive the throughput efficiency of this system.

22.6 Repeat Problem 22.5 for the go-back-N ARQ system.

22.7 Repeat Problem 22.5 for the ideal selective-repeat ARQ system.

22.8 Design a type-II hybrid ARQ system using a rate-1/3 convolutional code similar to the system presented in Section 22.7.

22.9 Let C be a half-rate invertible $(2k, k)$ systematic linear block code. Let $\mathbf{u}$ be an information sequence of k bits and $f(\mathbf{u})$ be its corresponding parity sequence. Prove that both $(\mathbf{u}, f(\mathbf{u}))$ and $(f(\mathbf{u}), \mathbf{u})$ are codewords in C.

22.10 Consider the RS outer code C_2 defined in Section 22.7. Prove that the parity word $R[\mathbf{v}(X)]$ given by (22.30) is also a codeword in C.

22.11 Design a type-II hybrid ARQ system in which a RS code C_2 over $GF(2^m)$ is used for forward error correction, and a half-rate RS code C_r obtained by shortening C_2 is used for parity retransmission. This is simply the hybrid system presented in Section 22.8 without an inner code.

22.12 The inner code C_1 of the hybrid system presented in Section 22.8 can be chosen as a binary (n, k) code designed for simultaneous error correction and detection. Design a concatenated hybrid ARQ system with C_1 as the inner code.

BIBLIOGRAPHY

1. R. J. Benice and A. H. Frey, Jr., "An Analysis of Retransmission Systems," *IEEE Trans. Commun. Technol.*, COM-12: 135–45, December 1964.