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

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

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 $|\mathbf{u}|\mathbf{u} + \mathbf{v}|$-construction.

4.13 Using the $|\mathbf{u}|\mathbf{u} + \mathbf{v}|$-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 $\mathbf{G} \cdot \mathbf{G}^T = 0$.)

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

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

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.