## PROBLEMS

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

$$v_0 = u_1 + u_2 + u_3,$$
$$v_1 = u_0 + u_1 + u_2,$$
$$v_2 = u_0 + u_1 + u_3,$$
$$v_3 = u_0 + u_2 + u_3.$$

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 $\mathbf{H}$ 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:

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

(Note that the last row of $\mathbf{H}_1$ 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 $v_\infty$, 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 $v_\infty$ 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 $\lambda$ 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 $\Gamma$ 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 $\Gamma$ or in none of the codes in $\Gamma$.

**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:

$$\mathbf{H} = \left[\begin{array}{c:c} & \mathbf{P}_1^T \\ \mathbf{I}_{n_1+n_2-k} & \mathbf{I}_k \\ & \mathbf{P}_2^T \end{array}\right].$$

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].)