Chapter 3

3.1 The generator and parity-check matrices are:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$|C_o| \leq |C_e| \tag{1}$$

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

$$C'_o \subseteq C_o$$

Hence

$$|C_e| \leq |C_o| \tag{2}$$

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

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

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

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

and

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

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

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

and

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

From (1) and (2), we obtain

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

From (3) and (4) ,we obtain

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

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

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

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

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

It is easy to see that

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

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

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

From the above inequality, we have

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

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

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

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

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

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

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

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

3.13 The generator matrix of the code is

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

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

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

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

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

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

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

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

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

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

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

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

This implies that

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

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

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

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

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

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

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

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

that

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

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

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

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

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