Solutions to selected problems from Chapter 3

3.1 The information sequences $\boldsymbol{u} = [u_0\ u_1\ u_2\ u_3]$ are encoded into codewords $\boldsymbol{v}$ of length $n = 8$, using a systematic encoder. If we assume that the systematic positions in a codeword are the *last* $k = 4$ positions, then codewords have the form

$$\boldsymbol{v} = [v_0\ v_1\ v_2\ v_3\ u_0\ u_1\ u_2\ u_3],$$

and the systematic encoding is specified by

$$\boldsymbol{v} = \boldsymbol{u}\boldsymbol{G}_{\text{sys}};\ \boldsymbol{G}_{\text{sys}} = [\,\boldsymbol{P}\ |\boldsymbol{I}\,].$$

From the given set of parity-check equations we immediately obtain the generator and the parity check matrices. For example, we can start with the parity check matrix $\boldsymbol{H}$ and recall that every row in $\boldsymbol{H}$ represents one parity-check equation, and it has ones on the positions corresponding to the symbols involved in that equation. Thus, we have

$$\boldsymbol{H}_{\text{sys}} = [\,\boldsymbol{I}\ |\boldsymbol{P}^{\mathrm{T}}\,] = \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right] \tag{1}$$

$$\boldsymbol{G}_{\text{sys}} = [\,\boldsymbol{P}\ |\boldsymbol{I}\,] = \left[\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \tag{2}$$

To find the minimum distance analytically, we use the property that the minimum distance of a binary linear code is equal to the smallest number of columns of the parity-check matrix $\boldsymbol{H}$ that sum up to zero (see Corollary 3.2.2 in the book). Hence, we find that:

- there are no two identical columns in $\boldsymbol{H}_{\text{sys}} \Rightarrow\ d_{\min} > 2$
- there are no groups of 3 columns that sum up to $\mathbf{0} \Rightarrow\ d_{\min} > 3$
- there exists a group of 4 columns (for example, columns 1,2,3,6) that sum up to $\mathbf{0} \Rightarrow\ \underline{d_{\min} = 4}$.

3.2 General structure of a systematic encoder for a linear (n, k) block code is shown in Figure 3.2 in the book. Based on the parity check equations from the previous problem, the systematic encoder for the $(8, 4)$ code has the structure as shown in Figure 1.

3.3 Syndrome vector is obtained from the received sequence $\boldsymbol{r} = [r_0\ r_1\ \ldots\ r_7]$ using the parity check matrix of the code:

$$\boldsymbol{s} = [s_0\ s_1\ s_2\ s_3] = \boldsymbol{r}\boldsymbol{H}^{\mathrm{T}}.$$

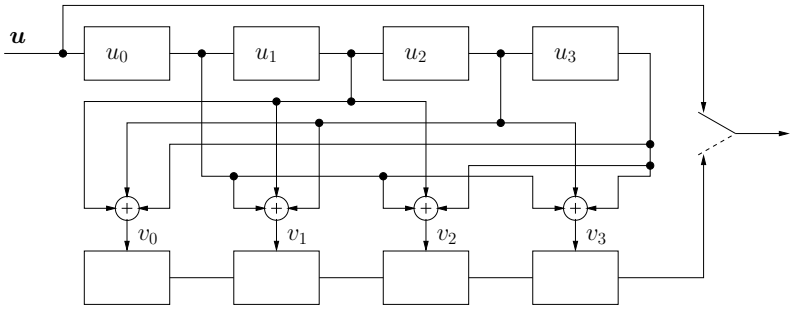

Figure 1: Systematic encoder for the $(8, 4)$ code.

By substituting the parity check matrix (1), we obtain that the syndrome digits are

$$\begin{aligned} s_0 &= r_0 + r_5 + r_6 + r_7 \\ s_1 &= r_1 + r_4 + r_5 + r_6 \\ s_2 &= r_2 + r_4 + r_5 + r_7 \\ s_3 &= r_3 + r_4 + r_6 + r_7. \end{aligned}$$

Using these equations the syndrome circuit is easily constructed following the general structure shown in Figure 3.4 in the book for any linear (n, k) block code.

3.4 (a) The parity check matrix $\boldsymbol{H}$ of a linear (n, k) code $\mathcal{C}$ has dimensions $(n-k) \times n$ and its rank is $n-k$ (all rows are linearly independent).
The matrix $\boldsymbol{H}_1$ has dimensions $(n-k+1) \times (n+1)$ and its rank is thus $\leq n-k+1$. Since $n-k$ rows of $\boldsymbol{H}$ are linearly independent, then, after adding a leading 0, these rows (the first $n-k$ rows of $\boldsymbol{H}_1$) are still independent. The last row of $\boldsymbol{H}_1$ begins with a 1, while the others begin with 0. Hence, we conclude that all rows of $\boldsymbol{H}_1$ are independent, and the rank of $\boldsymbol{H}_1$ is exactly $n-k+1$. Therefore, $\boldsymbol{H}_1$ is a parity check matrix of a code $\mathcal{C}_1$ whose dimension is the dimension of the null space of $\boldsymbol{H}_1$, that is, $\dim(\mathcal{C}_1) = (n+1) - (n-k+1) = k$.

(b)+(c) Extending the parity-check matrix $\boldsymbol{H}$ with a zero-column to the left and adding all-one row at the bottom is equivalent to adding the digit v_∞ to the left of each codeword of the original code $\mathcal{C}$, which is involved only in the last parity check equation specified by the all-one row, that is,

$$v_\infty + v_0 + v_1 + ... + v_{n-1} = 0.$$

This parity check equation implies that the weight, that is, the total number of ones in each codeword $[v_\infty\ v_0\ v_1\ ...\ v_{n-1}]$ of the extended code $\mathcal{C}_1$ must be *even*.
From the above parity check equation, it follows that the added digit v_∞ equals

$$v_\infty = \sum_{i=0}^{n-1} v_i.$$

Therefore, v_∞ is called the *overall parity check* digit: it equals 0 if the number of ones among the n symbols is even, otherwise it is equal to 1 (thus the total number of ones in the extended codeword is always even).

3.5 Let $\mathcal{C}_\mathrm{e}$ and $\mathcal{C}_\mathrm{o}$ be the subsets of a linear code $\mathcal{C}$, containing all the codewords with even and odd weight, respectively. Thus, $\mathcal{C}_\mathrm{e} \cap \mathcal{C}_\mathrm{o} = \emptyset$ and $\mathcal{C}_\mathrm{e} \cup \mathcal{C}_\mathrm{o} = \mathcal{C}$.

Let $\boldsymbol{v}$ be any odd-weight codeword from $\mathcal{C}_\mathrm{o}$. Then, if we add $\boldsymbol{v}$ to each codeword from $\mathcal{C}_\mathrm{o}$, we obtain a set $\mathcal{C}'_\mathrm{e}$ of even-weight words, which fulfills $|\mathcal{C}'_\mathrm{e}| = |\mathcal{C}_\mathrm{o}|$ (the number of elements in the two sets is the same). Also, it holds that $\mathcal{C}'_\mathrm{e} \subseteq \mathcal{C}_\mathrm{e}$, and thus

$$|\mathcal{C}'_\mathrm{e}| = |\mathcal{C}_\mathrm{o}| \leq |\mathcal{C}_\mathrm{e}|. \tag{3}$$

Similarly, if we add $\boldsymbol{v}$ to each codeword from $\mathcal{C}_\mathrm{e}$, we obtain a set $\mathcal{C}'_\mathrm{o}$ of odd-weight words, which fulfills $|\mathcal{C}'_\mathrm{o}| = |\mathcal{C}_\mathrm{e}|$. Also, it holds that $\mathcal{C}'_\mathrm{o} \subseteq \mathcal{C}_\mathrm{o}$, and thus

$$|\mathcal{C}'_\mathrm{o}| = |\mathcal{C}_\mathrm{e}| \leq |\mathcal{C}_\mathrm{o}|. \tag{4}$$

From (3) and (4) we conclude that

$$|\mathcal{C}_\mathrm{e}| = |\mathcal{C}_\mathrm{o}|,$$

and, since $|\mathcal{C}| = 2^k$, it follows that the number of odd-weight and even-weight codewords in a binary linear (n, k) code is

$$|\mathcal{C}_\mathrm{e}| = |\mathcal{C}_\mathrm{o}| = 2^{k-1}.$$

3.6 **(a)** The given condition on $\boldsymbol{G}$ ensures that, for any symbol position i, $0 \leq i < n$, there is a row in $\boldsymbol{G}$ with a non-zero symbol on that position. Since rows of the generator matrix are codewords of the code $\mathcal{C}$, we conclude that in the code array each column must contain at least one non-zero entry. Therefore, there are no all-zero columns in the code array.

(b) Consider an arbitrary ith column of the code array, $0 \leq i < n$, and let $\mathcal{S}_0$ and $\mathcal{S}_1$ be the sets of codewords that have a 0 and a 1 on the ith position, respectively. From part a) it follows that there is at least one codeword with a 1 on the ith position, that is, $|\mathcal{S}_1| \geq 1$. Now we follow an approach similar to the solution of Problem 3.5.

Let $\boldsymbol{v}$ be a codeword from $\mathcal{S}_1$. Then, if we add $\boldsymbol{v}$ to each codeword from $\mathcal{S}_1$, we obtain a set $\mathcal{S}'_0$ of codewords with a 0 on the ith position, and $|\mathcal{S}'_0| = |\mathcal{S}_1|$. Also, it holds that $\mathcal{S}'_0 \subseteq \mathcal{S}_0$, and thus

$$|\mathcal{S}'_0| = |\mathcal{S}_1| \leq |\mathcal{S}_0| \tag{5}$$

Similarly, if we add $\boldsymbol{v}$ to each codeword from $\mathcal{S}_0$, we obtain a set $\mathcal{S}'_1$ of words with a 1 on the ith position, which fulfills $|\mathcal{S}'_1| = |\mathcal{S}_0|$. Also, it holds that $\mathcal{S}'_1 \subseteq \mathcal{S}_1$, and thus

$$|\mathcal{S}'_1| = |\mathcal{S}_0| \leq |\mathcal{S}_1| \tag{6}$$

From (5) and (6) we conclude that

$$|\mathcal{S}_0| = |\mathcal{S}_1|.$$

Moreover, since $\mathcal{C} = \mathcal{S}_0 \cup \mathcal{S}_1$, $\mathcal{S}_0 \cap \mathcal{S}_1 = \emptyset$, and $|\mathcal{C}| = 2^k$, we conclude that

$$|\mathcal{S}_0| = |\mathcal{S}_1| = 2^{k-1},$$

that is, for any binary linear (n, k) code, exactly a half of codewords have a 0 and a half have a 1 on each position i, $0 \leq i < n$. Hence, each column in a code array has 2^{k-1} zeros and 2^{k-1} ones.

(c) For any two codewords $\boldsymbol{x}$ and $\boldsymbol{y}$ with a 0 on the ith position it holds that their sum is also a codeword with a 0 on the ith position, that is,

$$(\forall\, \boldsymbol{x}, \boldsymbol{y} \in \mathcal{S}_0) \quad \boldsymbol{x} + \boldsymbol{y} = \boldsymbol{z} \in \mathcal{S}_0.$$

Hence, $\mathcal{S}_0$ is a subspace (that is, a *subcode*) of the code $\mathcal{C}$. From part b) it follows that the dimension of this subspace is $k - 1$.

3.9 Let A_i denote the number of codewords of weight i in an (n, k) code $\mathcal{C}$. Then the numbers A_0, A_1, …, A_n are called the weight distribution of the code. For any linear code $A_0 = 1$ (every linear code must contain the all-zero codeword). The first next non-zero element of the weight distribution of a linear code is $A_{d_{\min}}$, corresponding to the number of minimal-weight codewords.

For the $(8, 4)$ code with the minimum distance $d_{\min} = 4$, all the codewords except the all-zero and the all-one codeword have minimum weight, that is, the weight distribution is

$$A_0 = 1;\ A_4 = 14;\ A_8 = 1.$$

When transmitting over binary symmetric channel (BSC), an undetected error event occurs when the error pattern is equal to some non-zero codeword. Thus, the probability of undetected error is (cf. expression (3.19) in the book)

$$P_u(E) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}$$

where p is the crossover probability of the BSC. For the $(8, 4)$ code we have

$$P_u(E) = A_4 p^4 (1-p)^{8-4} + A_8 p^8 (1-p)^{8-8} = 14p^4(1-p)^4 + p^8$$

which, for $p = 10^{-2} = 0.01$ yields

$$P_u(E) = 14 \cdot 10^{-8} 0.99^4 + 10^{-16} = 1.3448 \cdot 10^{-7}.$$

3.10 The optimum (maximum likelihood) decoder for the BSC is the minimum-distance decoder, which can be realized as a *standard array decoder*, or, more efficiently, as a *syndrome decoder*. For the $(8, 4)$ code, there are $2^{n-k} = 2^4 =$

16 different syndrome vectors. All-zero syndrome vector indicates that the transmission was either error-free, or an undetectable error has occurred (when the error pattern equals a codeword). Each syndrome corresponds to a coset of the code. Each coset has $2^k = 16$ sequences. The coset leader is the sequence with the smallest weight within the coset. The code itself is a coset with all-zero sequence as a coset leader and zero corresponding syndrome. Since the minimum distance of the $(8, 4)$ code is $d_{\min} = 4$, all single-error patterns are correctable, and simultaneously, all double-error events are detectable by a syndrome decoder. There are $\binom{8}{1} = 8$ single-error patterns and they are chosen as coset leaders of 8 cosets. These 8 cosets contain sequences of weights 1,3,5, and 7 (verify this!). The remaining $16 - 1 - 8 = 7$ cosets contain even-weight sequences. Thus, all $\binom{8}{2} = 28$ double-error patterns are in these 7 cosets and they are detectable via the corresponding 7 possible syndrome values. Double-error patterns chosen as coset leaders of these 7 cosests will be correctable, but it cannot be guaranteed that *all* double errors will be corrected. However, since all double error patterns belong to the cosets distinct from cosets whose leaders are single-error patterns, it is guaranteed that the decoder will simultaneously detect double errors and correct single errors.

The decoder operates as follows: first, it computes the syndrome $\boldsymbol{s} = \boldsymbol{r}\boldsymbol{H}^{\mathrm{T}}$. Then, a coset leader whose syndrome is equal to the obtained value is located (for example, a look-up table can be used for this mapping). If the syndrome is zero, it is assumed that no errors occurred and the decoder outputs $\hat{\boldsymbol{v}} = \boldsymbol{r}$. If the syndrome is non-zero and the corresponding coset leader is a weight-one sequence $\boldsymbol{e}$, this sequence is chosen as the assumed error pattern that occurred on the channel and the decoded codeword is $\hat{\boldsymbol{v}} = \boldsymbol{r} + \boldsymbol{e}$. If the computed syndrome corresponds to the coset leader of weight larger than 1, this is an indicator that at least 2 errors occurred on the channel.

3.12 See solution of Problem 3.10. The syndrome decoder explained in the previous solution is the optimum decoder. It will correct all 8 single errors and 7 double errors that are chosen as coset leaders (the choice is not unique!). The all-zero syndrome is interpreted as error-free transmission.

3.15 ***Hamming bound:*** For any binary (n, k) linear block code with minimum distance of at least $2t + 1$ (for some positive integer t), it holds

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

Proof: According to Theorem 3.5 from the book, an (n, k) code with minimum distance $2t + 1$ or greater can correct all errors of weight up to t with the syndrome decoder whose coset leaders are the sequences of up to t ones. There are

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

such sequences. On the other hand, there are 2^{n-k} diferrent cosets, and this number cannot be smaller than the number of coset leaders (correctable error patterns). Thus we have

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

Taking the logarithm $\log_2$ of both sides of the above inequality yields the Hamming bound, which completes the proof.

3.16 ***Plotkin bound:*** The minimum distance of an (n, k) linear code satisfies

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

Proof: Consider the $2^k \times n$ code array whose rows are codewords of the (n, k) code $\mathcal{C}$. Each column of this array contains exactly 2^{k-1} zeros and 2^{k-1} ones (see Problem 3.6). Hence, the total number of ones in the code array is $n \cdot 2^{k-1}$. On the other hand, each of the $2^k - 1$ non-zero codewords has weight of at least $d_{\min}$. Hence, the total number of ones in the code array is at least $(2^k - 1)d_{\min}$. By combining these two results we obtain

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

which yields the Plotkin bound

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

3.17 ***Theorem:*** There exists an (n, k) linear code with a minimum distance of at least d if

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

Proof:

The number of non-zero 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 $2^{(k-1)(n-k)}$ linear codes. Therefore, there are at most $M = 2^{(k-1)(n-k)} \sum_{i=1}^{d-1} \binom{n}{i}$ linear codes that contain nonzero codewords of weight $d - 1$ or less.

On the other hand, the number of different $k \times n$ binary generator matrices in systematic form is $2^{k(n-k)}$, which means that $N = 2^{k(n-k)}$ is the total number

of binary linear codes. If $M < N$, there exists at least one code with minimum codeword weight at least d. Condition $M < N$ is equivalent to

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

which yields

$$\sum_{i=1}^{d-1} \binom{n}{i} < 2^{n-k}. \tag{7}$$

3.18 ***Gilbert-Varshamov bound:***

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

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

(The right-hand side of this inequality is known as Gilbert-Varshamov bound and provides lower bound on the minimum distance attainable with an (n, k) linear code).

Proof: The proof follows directly from Problem 3.17. Namely, let $d_{\min}$ be the largest positive integer such that the inequality (7) holds. Then, for this $d_{\min}$ it holds:

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

According to Problem 3.17, if the the left part of the above inequality is fulfilled, there exists a linear code of minimum distance at least $d_{\min}$.

3.20 A codeword of an $(n, n-1)$ single parity check code consists of $n-1 = k$ information symbols followed by an overall parity bit $v_{n-1} = p = \sum_{i=0}^{k-1} u_i$. The encoder can be realized using a single memory element, as shown in Figure 2. The memory element is initially in the zero state. During the encoding it contains the current parity of the information sequence. After k clocks, at the output of the memory element appears the overall parity bit p which is sent after the information block.

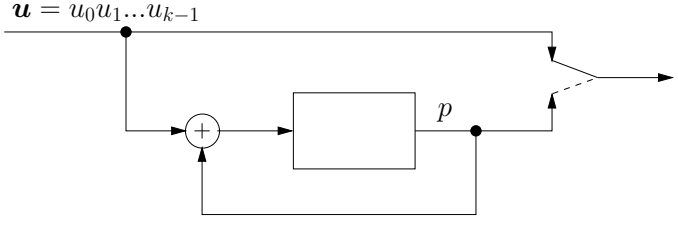

Figure 2: Encoder for the $(n, n-1)$ single parity check (SPC) code.