Solutions 5

Exercise 5.1.

1. First, note that G has rank k, because of the triangular minor it contains. Moreover, the rows of G, when interpreted as polynomials, represent $g(x), xg(x), \ldots, x^{k-1}g(x)$ which form a basis for the ideal in $\mathbb{F}_2[x]/(x^n - 1)$ generated by $g(x)$, i.e., the code $\mathcal{C}$.

2. For any codeword $c(x) = \sum_{i=0}^{n-1} c_i x^i$, we can write $c(x) = f(x)g(x)$ for some polynomial $f(x)$ of degree less than $n - k$. Then

$$c(x)h(x) = f(x)g(x)h(x) = 0 \pmod{x^n - 1}.$$

The coefficient of x_j in this product is

$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0,\ j = 0, \ldots, n-1, \tag{1}$$

where the subscripts are taken modulo n. This gives us n check equations satisfied by the codewords of $\mathcal{C}$. Let

$$H := \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}$$

Clearly, from (1), if $c \in \mathcal{C}$ then $Hc^\top = 0$. Conversely, note that H has rank $n-k$ because of the triangular minor it contains, so that the codition $Hc^\top = 0$ is a sufficient condition for c to be in $\mathcal{C}$. Thus H is a parity check matrix for $\mathcal{C}$.

3. From $g(x)h(x) = x^7 - 1$, we get that $h(x) = x^4 + x^2 + x + 1$, and thus by the result in the preceding section, we will have

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

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

This code is equivalent to a $[7, 4, 3]$ Hamming code (i.e., it is the Hamming code up to a permutation of the codeword coordinates).

Exercise 5.2.

1. As n is relatively prime to the field size, $x^n - 1$ has no duplicate factors and thus $\gcd(g(x), h(x)) = 1$. Now we can apply Bezout's identity and conclude that there exist $a(x)$ and $b(x)$ such that $a(x)g(x) + b(x)h(x) = \gcd(g(x), h(x)) = 1$.

2. We have that $c(x) := a(x)g(x) = 1 - b(x)h(x)$. Thus, for every codeword $f(x)$, we will have
$$c(x)f(x) = f(x) - b(x)f(x)h(x) = f(x).$$
In particular, letting $f(x) = c(x)$, we get that $c(x)^2 = c(x) \mod x^n - 1$. Also, since we know that every codeword $w(x)$ of $\mathcal{C}$ can be written as a multiple of $c(x)$, namely, $w(x)c(x)$, it follows that $c(x)$ generates $\mathcal{C}$.

   For the uniqueness, assume that there is a codeword $c'(x)$ such that for all codewords $f(x)$ of $\mathcal{C}$, $f(x)c'(x) = f(x)$. Now let $f(x) = c(x)$; thus, $c(x)c'(x) = c(x)$. Similarly, c having the same property implies that $c'(x)c(x) = c'(x)$, which gives $c(x) = c'(x)$.

Exercise 5.3.

1. If $c \in \mathcal{C}_1 \cap \mathcal{C}_2$ and c' is any cyclic shift of c, we must have that $c \in \mathcal{C}_1$ thus $c' \in \mathcal{C}_1$ and similarly, $c' \in \mathcal{C}_2$, which means $c' \in \mathcal{C}_1 \cap \mathcal{C}_2$ and that $\mathcal{C}_1 \cap \mathcal{C}_2$ is cyclic. For the generator polynomial, let $g(x) = \mathrm{LCM}(g_1(x), g_2(x))$; the least common multiple of $g_1(x)$ and $g_2(x)$. Every codeword in the intersection is divisible by both $g_1(x)$ and $g_2(x)$, and thus, by $g(x)$. Conversely, every multiple of $g(x)$ is both a multiple of $g_1(x)$ and $g_2(x)$ and must belongs to both codes. This means that $\mathcal{C}_1 \cap \mathcal{C}_2$ is generated by $g(x)$.

2. Let $c := c_1 + c_2 \in \mathcal{C}_1 + \mathcal{C}_2$, where $c_1 \in \mathcal{C}_1$ and $c_2 \in \mathcal{C}_2$, and consider a cyclic shift of c, denoted by c', and corresponding cyclic shifts of c_1 and c_2 denoted by c'_1 and c'_2, respectively. We must have that $c' = c'_1 + c'_2$, and c'_1 (resp., c'_2) must belong to $\mathcal{C}_1$ (resp., $\mathcal{C}_2$) by the properties of $\mathcal{C}_1$ and $\mathcal{C}_2$. This means that $c' \in \mathcal{C}_1 + \mathcal{C}_2$ and thus $\mathcal{C}_1 + \mathcal{C}_2$ is cyclic. Now consider the polynomial $g(x) = \gcd(g_1(x), g_2(x))$. First we observe that every multiple of $g_1(x)$ or $g_2(x)$ is a multiple of $g(x)$ as well, which means that the code generated by $g(x)$ contains both $\mathcal{C}_1$ and $\mathcal{C}_2$ and hence $\mathcal{C}_1+\mathcal{C}_2$. Now, by Bezout's identity,
$$g(x) = a(x)g_1(x) + b(x)g_2(x) \mod x^n - 1$$
for some $a(x), b(x)$, so that every multiple of $g(x)$ (e.g., $g(x)u(x)$) can be written as the summation $a(x)u(x)g_1(x) + b(x)u(x)g_2(x)$ which is a multiple of $g_1(x)$ plus a multiple of $g_2(x)$. Thus the code generated by $g(x)$ is contained in $\mathcal{C}_1 + \mathcal{C}_2$. We conclude that $\mathcal{C}_1 + \mathcal{C}_2$ is the cyclic code generated by $g(x)$.

Exercise 5.4.

1. Suppose that λ is a nonzero linear form on $\mathbb{F}_2^k$. Its image is nontrivial, so that its kernel has dimension $k-1$; this means that λ vanishes on exactly half the points of $\mathbb{F}_2^k$. Thus the solution spaces of $\lambda(x) = 0$ and $\lambda(x) = 1$ have equal size.

2. By the definition of the ϵ-biased set, in each codeword of the evaluation code the number of zeros and ones differ by at most $\epsilon|S|$. As the length of the code of $|S|$, each codeword will have weight (thus, the code will have minimum distance) at least $(1-\epsilon)|S|/2$. In particular, the left kernel of a generator matrix of the code whose columns form the set S must be trivial, which means that the dimension of the code is k.

3. As the all-one word is a codeword and the code is linear, the weight distribution of the code is symmetric; i.e., there is a codeword of weight i in the code iff there is one of weight $n - i$. Now let G' be the generator matrix G with its first row removed and S be the set of its n columns. Thus, G' is a generator matrix of a subcode of $\mathcal{C}$ that does not contain the all-one word. We know that for each nonzero $x \in \mathbb{F}_2^{k-1}$, the weight of $y := xG'$ is in the range $[d, n - d]$. Let n_0 and n_1 be the number of zeros and ones in y. Thus we know that $n_0 + n_1 = n$ and $n_0, n_1 \in [d, n - d]$, which means $|n_0 - n_1| \leq n - 2d = (1 - 2d/n)|S|$. Note that the choices of x are in one-to-one correspondence with nonzero elements of $(\mathbb{F}_2^{k-1})^*$ and the outcomes y are in one-to-one correspondence with evaluation table of nonzero linear forms over the set S. This means that the set S is ϵ-biased, for $\epsilon = 1 - 2d/n$.