Exercise Sheet 5

Exercise 5.1. Suppose that $\mathcal{C}$ is a cyclic code of length n over $\mathbb{F}_2$ generated by a polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$.

1. Show that the $k \times n$ matrix G below is a generator matrix for C.

$$G := \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

2. Define the *check polynomial* $h(x)$ as $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ where $x^n - 1 = g(x)h(x)$. For any codeword $c(x)$, what can be said about $c(x)h(x)$? Write down a check matrix for $\mathcal{C}$.

3. Let $\mathcal{C}$ be a cyclic code of length 7 over $\mathbb{F}_2$ with a generator polynomial $g(x) = x^3 + x + 1$. Compute the check polynomial and generator and parity check matrices for the code. What is this code called?

Exercise 5.2. Let $\mathcal{C}$ be a cyclic code of length n over $\mathbb{F}_2$ (where n is odd) generated by a polynomial $g(x)$, and denote by $h(x)$ the check polynomial, i.e., $g(x)h(x) = x^n - 1$.

1. Show that there are polynomials $a(x)$ and $b(x)$ such that $a(x)g(x) + b(x)h(x) = 1$.

   [Hint: recall the following fact: since n and the field size 2 are relatively prime, $x^n - 1$ has n distinct zeros (living in an extension field $\mathbb{F}_2^m$).]

2. Let $c(x) := a(x)g(x)$ be a codeword of $\mathcal{C}$, where $a(x)$ is as defined in 1. Show that for any codeword $f(x)$ of $\mathcal{C}$, we have

$$c(x)f(x) = f(x) \mod x^n - 1,$$

   and that $c(x)$ is the unique codeword of $\mathcal{C}$ with this property. Conclude that $c(x)$ generates $\mathcal{C}$ and that

$$c(x)^2 = c(x) \mod x^n - 1.$$

Exercise 5.3. Count the number of linear cyclic codes of length 8 over $\mathbb{F}_3$.

Exercise 5.4. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be cyclic codes of length n generated by polynomials $g_1(x)$ and $g_2(x)$, respectively, over $\mathbb{F}$. Show that the following codes are cyclic and find their generator polynomials:

1. $\mathcal{C}_1 \cap \mathcal{C}_2$.

2. $\mathcal{C}_1 + \mathcal{C}_2 := \{c_1 + c_2 : c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2\}$.

Exercise 5.5. A set $S \subseteq \mathbb{F}_2^k$ is called ϵ-biased (for some $\epsilon \in [0,1)$) if

$$\forall \lambda \in (\mathbb{F}_2^k)^*, \lambda \neq 0 \colon \qquad \big|\, \#\{x \in S \mid \lambda(x) = 0\} - \#\{x \in S \mid \lambda(x) = 1\} \,\big| \leq \epsilon |S|.$$

1. Show that $\mathbb{F}_2^k$ is 0-biased.
2. Show that if S is ϵ-biased, then the evaluation code with parameters (V, S), $V = \left(\mathbb{F}_2^k\right)^*$, has minimum distance $\geq \frac{(1-\epsilon)}{2}|S|$ and dimension k.
3. Let $\mathcal{C}$ be an $[n, k, d]_2$-code which contains the all-one vector, and G be a generator matrix for $\mathcal{C}$ whose first row is the all-one vector. Show that the columns of G with its first row removed form an ϵ-biased set with $\epsilon = 1 - 2d/n$.