Exercise Sheet 5

Exercise 5.1. A set $S \subseteq \mathbb{F}_2^k$ is called ϵ-biased if

$$\forall \lambda \in \left(\mathbb{F}_2^k\right)^* : \quad \left| \#\{x \in S \mid \lambda(x) = 0\} - \#\{x \in S \mid \lambda(x) = 1\} \right| \leq \epsilon |S|.$$

(a) Show that $\mathbb{F}_2^k$ is 0-biased.

(b) Show that if S is ϵ-biased, then the evaluation code with parameters (V, S), $V = \left(\mathbb{F}_2^k\right)^*$, has dimension k and minimum distance $\geq \frac{(1-\epsilon)}{2}|S|$.

(c) Show that if C is an $[n, k, d]_2$-code which contains the all-one vector, then the columns of any generator matrix of C form an ϵ-biased set with $\epsilon = 1 - 2d/n$.

Exercise 5.2. Let C be an irreducible binary cyclic code, i.e., a binary cyclic code that has no nontrivial cyclic subcode. Show that all weights in C are even.

Exercise 5.3. Suppose that $\mathcal{C}$ is a cyclic code of length n over $\mathbb{F}_2$ generated by a polynomial $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$, where $x^n - 1 = g(x)h(x)$ and $h(x) = h_0 + h_1 x + \cdots + h_k x^k$ is the parity check polynomial.

1. Show that the matrices G and H below are generator and parity check matrices for $\mathcal{C}$:

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