Exercise Sheet 2

Exercise 2.1. Let $c \in \mathbb{F}_2^n$ be of weight d. What is the number of binary vectors of weight w that are orthogonal to c? (*Hint:* Use MacWilliams identities.)

Exercise 2.2. In this exercise, we will look at two common procedures for creating new codes from old ones.

1. **Puncturing.** Let C be an $[n, k, d]_q$-code. The *punctured code at position i*, denoted C^i, is the set of words $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ of length $n-1$ formed by removing the ith coordinate of each codeword. Show that C^i is a linear code. What are its parameters?
2. **Shortening.** Let C be an $[n, k, d]_q$-code. The *shortened code C_i* is formed as follows: let C' be the intersection of C with the hyperplane $\{x \in \mathbb{F}_q^n : x_i = 0\}$. C_i is then formed by puncturing C' at position i. Show that C_i is a linear code. What are its parameters?
3. Show that
$$(C^\perp)_i = (C^i)^\perp.$$

Exercise 2.3. The *extended Hamming code* is constructed as follows: start with the $[7, 4, 3]_2$-Hamming code and add a position to each codeword. In that position, put a 1 if the codeword is of odd weight, and put a 0 otherwise.

1. Show that the extended Hamming code is an $[8, 4, 4]_2$-code and find a generator and a check matrix for this code.
2. Show that the dual of the extended Hamming code is equal to the code itself.

Exercise 2.4. An $[n, k, d]_q$-code is called *perfect* if the Hamming balls of radius $(d-1)/2$ around the codewords form a disjoint union of $\mathbb{F}_q^n$. Show that binary Hamming codes are perfect.

Exercise 2.5. Given integers $N \leq n$, $K \geq k$, and $D \geq d$, show that if there is no $[n, k, d]_q$-code, then there is no $[N, K, D]_q$-code.

Exercise 2.6. Let d be an odd positive integer. Show that there is a $[n, k, d]_2$-code iff there is an $[n+1, k, d+1]_2$-code.

Exercise 2.7. Let $A_q(n, d)$ be the maximum k for which an $[n, k, d]_q$-code exists. Show that $A_2(n, 2) = n - 1$.

Exercise 2.8. Let $\mathcal{C}$ be an $[n, k]$ code over $\mathbb{F}_q$.

1. Show that the minimum distance of $\mathcal{C}$ is the largest integer d such that every $k \times (n - d + 1)$ submatrix of its generator matrix has rank k.
2. Show that $\mathcal{C}$ is MDS if and only if its dual is.

Exercise 2.9. Let $\mathcal{C}$ be a perfect (n, M, d) code (with $d = 2t + 1$) over $\mathbb{F}_q$ and suppose that $\mathcal{C}$ contains the all zero codeword. Show that the number of codewords of Hamming weight $2t + 1$, denoted W_{2t+1} is given by

$$W_{2t+1} = \frac{\binom{n}{t+1} \cdot (q-1)^{t+1}}{\binom{2t+1}{t}}$$

Hint : Given a codeword c of Hamming weight $2t + 1$ in $\mathcal{C}$, show that there are exactly $\binom{2t+1}{t}$ words of Hamming weight $t + 1$ in $\mathbb{F}_q^n$ that are decoded to c by nearest-neighbor decoding.

Exercise 2.10. You are given twelve coins and a balance. One of the coins might be counterfeit (*i.e.* its weight is larger or smaller than the others). Your balance can only compare two heaps of coins. Give a procedure to identify the fake coin after three weightings.