Exercise Sheet 3

Exercise 3.1. The *hexacode* $\mathcal{G}_6$. We consider the field $\mathbb{F}_4 = \mathbb{F}_2[\omega]$, where $\omega^2+\omega+1 = 0$, equiped with the conjugation $x \mapsto \overline{x}$ where $\overline{\omega} = \omega^2$. The Hermitian inner product is $x \cdot y = \sum_{i=1}^{n} x_i \overline{y_i}$. The hexacode $\mathcal{G}_6$ is the quaternary code

$$\mathcal{G}_6 = \{(a, b, c, f(1), f(\omega), f(\omega^2)); (a, b, c) \in \mathbb{F}_4^3, f(x) = cx^2 + bx + a\}$$

1. Give a generator matrix of $\mathcal{G}_6$. What are the length, dimension and minimal distance of $\mathcal{G}_6$? What can you say about $\mathcal{G}_6$?
2. Show that $\mathcal{G}_6$ is Hermitian self-dual.
3. Prove that any code with the same parameters than $\mathcal{G}_6$ is equivalent to the hexacode, *i.e.* equal to $\mathcal{G}_6$ up to permutation of coordinates and multiplications of the coordinates by a scalar.

Exercise 3.2. Let $\mathcal{C}$ be a binary linear code. Prove that

1. If $\mathcal{C}$ is self-orthogonal and has a generator matrix each of whose rows has weight divisible by four, then every codeword of $\mathcal{C}$ has weight divisible by four.
2. If every codeword has weigth divisible by four, then $\mathcal{C}$ is self-orthogonal.

Exercise 3.3. Let $\mathcal{G}_{24}$ be the $[24, 12]_2$-code with generator matrix $G_{24} = [\mathrm{I}_{12}|A]$ where

$$A = \left(\begin{array}{c|cccccccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

Assume the row and colums of A are indexed by $\infty, 0, 1, \ldots, 10$, notice that then the coefficient of in position (i, j) (i j finite) is 1 if $i + j$ is a square in $\mathbb{F}_{11}$ and 0 otherwise.

1. Show that $\mathcal{G}_{24}$ is self-dual.
2. Prove that $[A|\mathrm{I}_{12}]$ is also a generator matrix of $\mathcal{G}_{24}$, deduce that $(a, b) \in \mathcal{G}_{24}$ iff $(b, a) \in \mathcal{G}_{24}$ for $a, b \in \mathbb{F}_2^{12}$. Prove that there is no codeword of weight 4. Show that the minimal distance of $\mathcal{G}_{24}$ is 8.

3. Prove that there exist a $[23, 12, 7]_2$-code.

The code $\mathcal{G}_{24}$ is called the *extended binary Golay code*. The $[23, 12, 7]_2$-code you obtained is called the *binary Golay code*.

With more work, it is possible to show that any binary code of length 23 and 24, possibly non linear, each containing $\mathbf{0}$, $M \geq 2^{12}$ codewords and minimum distance 7 and 8 are actually unique and equal to a Golay code. (See *e.g* W. Cary Huffman and Vera Pless, *Fondamentals of Error-Correcting Codes*, Cambridge 2003)

Exercise 3.4. Let $\mathcal{C}$ be a linear $[n, k > 1, d]$ code over $\mathbb{F}_q$ with a generator matrix of the form

$$G = \left(\begin{array}{cccc|cccc} 0 & 0 & \dots & 0 & 1 & 1 & \dots & 1 \\ \multicolumn{4}{c|}{G_1} & \multicolumn{4}{c}{G_2} \end{array} \right),$$

where the Hamming weight of the first row is d. Define $\mathcal{C}_1$ as the linear $[n_1 := n - d, k_1, d_1]$-code over $\mathbb{F}_q$ generated by G_1.

1. Show that G_1 has rank $k - 1$, and thus, $k_1 = k - 1$.
2. Let c_1 be a codeword of $\mathcal{C}_1$. Show that the number of words $c_2 \in \mathbb{F}_q^d$ such that $(c_1 \mid c_2) \in \mathcal{C}$ is exactly q, and that if c_1 is nonzero, there is such a choice for c_2 with Hamming weight at most $d - \lceil d/q \rceil$.
3. Show that $d_1 \geq \lceil d/q \rceil$.

Exercise 3.5. Denote by $N_q(k, d)$ the length of a shortest linear code of dimension k and distance d over $\mathbb{F}_q$.

1. Show that $N_q(k, d) \geq d + N_q(k - 1, \lceil d/q \rceil)$. (*Hint:* use the last exercise.)
2. Show that $N_q(k, d) \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. Derive the Singleton bound for linear codes using this result.
3. Show that the first-order Reed-Muller code over $\mathbb{F}_q$ achieves this bound. Recall that the first-order Reed-Muller code is defined as the linear $[q^m, m + 1]$-code over $\mathbb{F}_q$ with an $(m + 1) \times q^m$ generator matrix whose columns range over all the vectors in $\mathbb{F}_q^{m+1}$ with a first entry equaling 1.

Exercise 3.6. A *burst of length* ℓ is the event of having errors in a codeword such that the locations i and j of the first (leftmost) and last (rightmost) errors, respectively, satisfy $j - i = \ell - 1$. Let $\mathcal{C}$ be a linear $[n, k]$-code over $\mathbb{F}_q$ that is able to correct every burst of length t or less.

1. Show that in every nonzero codeword $c \in \mathcal{C}$, the locations i and j of the first and last nonzero entries in c must satisfy $j - i \geq 2t$.
2. Show that $n - k \geq 2t$.
3. (Sphere-packing:) Show that

$$q^{n-k} \geq 1 + n(q - 1) + (q - 1)^2 \sum_{i=0}^{t-2} (n - i - 1)q^i.$$