Exercise 1. Weight distribution of some self-dual code
Let $C \subseteq \mathbb{F}_q^n$ be a self-dual code, i.e., $C = C^\perp$.

1. Show that the length $n$ of $C$ is even and that its dimension equals $\frac{n}{2}$.

2. Show that all codewords in a binary self-dual code have an even Hamming weight.

3. Let $C$ be a binary self-dual code of length 6. Show that its weight enumerator has the following form
$$P_C(x, y) = y^6 + a_2x^2y^4 + a_4x^4y^2 + a_6x^6$$
with $a_6 \in \{0, 1\}$ and $1 + a_2 + a_4 + a_6 = 8$.

4. Deduce from MacWilliams’ formula that such a code contains the all-one word.

5. Deduce that $a_2 = a_4$.


Exercise 2. Griesmer bound
Let $C$ be a linear binary code of length $n$, dimension $k$ and minimum distance $d$. W.l.o.g. we assume that the word $c = (1 \cdots 1 0 \cdots 0)$ of weight $d$ defined by $c_1 = \cdots = c_d = 1$ and $c_{d+1} = \cdots = c_n = 0$ belongs to $C$ (otherwise, the coordinates of the code can be permuted, since it does not influence the weight distribution). Let $p$ be the mapping defined by
$$p : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{n-d}, \quad (x_1, \ldots, x_n) \mapsto (x_{d+1}, \ldots, x_n).$$

1. Prove that $c$ is the unique word in $C \setminus \{0\}$ such that $p(c) = 0$.

2. Prove that the image $C'$ of $C$ by $p$ has dimension $k - 1$.

3. Let $d'$ be the minimum distance of $C'$. Let $v \in C$ be a word such that $p(v) \in C'$ has weight $d'$. Let $a = w_H(v) - d'$. Prove that
   (i) $a + d' \geq d$;
   (ii) $d - a + d' \geq d$.

4. Deduce that $d' \geq \frac{d}{2}$.

5. Show that, for any binary code $C$ with parameters $[n, k, d]$, we have
$$n \geq \sum_{i=0}^{k-1} \frac{d}{2^i}. \quad (1)$$

6. Exhibit a generator matrix of a binary $[6, 2, 4]$-code, and a generator matrix of a binary $[9, 2, 6]$-code. More generally, prove that the Griesmer bound (1) is optimal for $k = 2$ and $n$ multiple of 3.
7. Let $(C_\ell)_{\ell \in \mathbb{N}}$ be a sequence of codes with parameters $[n_\ell, k_\ell, d_\ell]$ such that $(n_\ell)_\ell$ and $(k_\ell)_\ell$ tend to infinity and $(d_\ell/n_\ell)_\ell$ converges to some integer $\delta$. Prove that $\delta \leq \frac{1}{2}$.

8. Is this result more or less accurate than the asymptotic Plotkin bound?

**Exercise 3. Extended Reed-Solomon Codes**

Let $\alpha = (\alpha_1, \ldots, \alpha_q) \in \mathbb{F}_q^q$ be such that the $\alpha_i$’s are pairwise distinct. That is, the set of elements of $\mathbb{F}_q$ is $\{\alpha_1, \ldots, \alpha_q\}$. Let $k \leq q$ be an integer and $\mathbb{F}_q[z]_{<k}$ be the space of polynomials of degree strictly less than $k$. For all $f \in \mathbb{F}_q[z]_{<k}$, we define $\text{ev}_{\infty,k-1}(f)$, the *evaluation at infinity of $f$* as $\text{ev}_{\infty,k-1}(f) := (z^{k-1}f(1/z))_{z=0}$.

Let $\text{ERS}_k(\alpha)$ be the Extended Reed Solomon (ERS) code defined as the image of the linear map

$$
\mathbb{F}_q[z]_{<k} \rightarrow \mathbb{F}_q^{q+1}
$$

$$
f \mapsto (f(\alpha_1), \ldots, f(\alpha_q), \text{ev}_{\infty,k-1}(f)).
$$

1. Prove that for all $f \in \mathbb{F}_q[z]_{<k}$, $\text{ev}_{\infty,k-1}(f)$ is the coefficient $f_{k-1}$ of $x^{k-1}$ in $f$.
2. Prove that $\text{ERS}_k(\alpha)$ is MDS.
3. Prove that the dual of an ERS code is an ERS code.

**Exercise 4. Minimum-weight codewords in MDS codes**

Let $C$ be an $[n, k, d]$-code over $\mathbb{F}_q$. Prove that $C$ is MDS if and only any subset of $\{1, \ldots, n\}$ of size $d$ is the support of a codeword in $C$. 

2