EXERCISES N° 3, MDS AND REED–SOLOMON CODES

Exercise 1 (Singleton bound for nonlinear codes)**.** Let $C \subset \mathbb{F}_q^n$ be a nonlinear code of minimum distance d. Prove that

$$|C| \leqslant q^{n-d+1}.$$

Indication: use the restriction to C of the map $\left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ x & \longmapsto & (x_d, \dots, x_n) \end{array} \right.$.

Exercise 2 (Extended Reed–Solomon Codes)**.** Let $\alpha \stackrel{\text{def}}{=} (\alpha_1, \dots, \alpha_q) \in \mathbb{F}_q^n$ be such that the α_i's are pairwise distinct. That is, the set of elements of $\mathbb{F}_q$ is $\{\alpha_1, \dots, \alpha_q\}$. Let $k \leqslant q$ 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 $\mathrm{ev}_{\infty,k-1}(f)$, the *evaluation at infinity of f* as $\mathrm{ev}_{\infty,k-1}(f) := \left(z^{k-1} f(1/z)\right)_{z=0}$ Let $\mathbf{ERS}_k(\alpha)$ be the Extended Reed Solomon (ERS) code defined as the image of the linear map

$$\left\{ \begin{array}{ccc} \mathbb{F}_q[z]_{<k} & \longrightarrow & \mathbb{F}_q^{q+1} \\ f & \longmapsto & (f(\alpha_1), \dots, f(\alpha_q), \mathrm{ev}_{\infty,k-1}(f)) \end{array} \right. .$$

(1) Prove that for all $f \in \mathbb{F}_q[z]_{<k}$, $\mathrm{ev}_{\infty,k-1}(f)$ is the coefficient f_{k-1} of x^{k-1} in f. In particular, it is 0 if and only if f has degree $< k-1$.
(2) Prove that $\mathbf{ERS}_k(\alpha)$ is MDS.
(3) Prove that the dual of an ERS code is an ERS code.

Exercise 3 (Higher weights)**.** Let $C \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$ code. Let $\mathcal{I} = \{i_1, \dots, i_r\} \subseteq \{1, \dots, n\}$. Recall that the shortening of C at $\mathcal{I}$ is defined as

$$\mathcal{S}_{\mathcal{I}}(C) \stackrel{\text{def}}{=} \left\{(c_{i_1}, \dots, c_{i_r}) \mid c \in C, \text{ such that } \forall i \notin \mathcal{I},\ c_i = 0\right\}.$$

Let $1 \leqslant r \leqslant k$, we denote the r–th generalised Hamming weight d_r of C as the minimal size of a subset $\mathcal{I} \subseteq \{1, \dots, n\}$ such that the subcode of words whose support is contained in $\mathcal{I}$ has dimension r. That is,

$$d_r \stackrel{\text{def}}{=} \min\left\{|\mathcal{I}| \;\middle|\; \dim \mathcal{S}_{\mathcal{I}}(C) = r\right\}.$$

(1) Prove that d_1 is nothing but the minimum distance d of C.
(2) Prove that the sequence $d_1, d_2, \dots, d_k$ is strictly increasing.
(3) Prove that if C is an $[n, k, d]$ Reed-Solomon code, then for all $i \leqslant k$,

$$d_i = n - k + i.$$

(4) Prove that the previous result actually holds for every MDS code.
Indication : First prove that every shortening of an MDS code is MDS.

Exercise 4 (Hamming isometries)**.** The goal of this exercise is to classify the set of Hamming isometries of $\mathbb{F}_q^n$, that is the set of maps $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that

$$\forall x, y \in \mathbb{F}_q^n,\ d_H(\varphi(x), \varphi(y)) = d_H(x, y),$$

where d_H denotes the Hamming distance.

(1) Prove that isometries are bijective and that the set $\mathbf{Isom}(\mathbb{F}_q^n)$ of isometries of $\mathbb{F}_q^n$ is a group for the composition law.

(2) We first focus on **linear** isometries of $\mathbb{F}_q^n$. Let $\mathbf{Aut}(\mathbb{F}_q^n)$ be the subgroup of $\mathbf{Isom}(\mathbb{F}_q^n)$ of linear isometries of $\mathbb{F}_q^n$. These isometries are represented by $n \times n$ matrices. Let $\mathbf{D}_n$ be the group of invertible diagonal matrices and $\mathfrak{S}_n$ be the group of permutation matrices.

   (a) Prove that $\mathbf{D}_n$ and $\mathfrak{S}_n$ are subgroups of $\mathbf{Aut}(\mathbb{F}_q^n)$.

   (b) Prove that $\mathbf{Aut}(\mathbb{F}_q^n)$ is spanned by $\mathbf{D}_n$ and $\mathfrak{S}_n$.

   More precisely (stop the question here if you don't know anything about the semi-direct product), prove that

$$\mathbf{Aut}(\mathbb{F}_q^n) = \mathbf{D}_n \rtimes \mathfrak{S}_n$$

   where the action of $\mathfrak{S}_n$ on $\mathbf{D}_n$ is the action by permutation on the diagonal coefficients.

(3) Let $u \in \mathbb{F}_q^n$, prove that the translation by u :

$$t_u : \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ x & \longmapsto & x+u \end{array} \right.$$

is an isometry.

(4) Let $\mathbf{Isom}_0(\mathbb{F}_q^n)$ be the subgroup of $\mathbf{Isom}(\mathbb{F}_q^n)$ of isometries sending 0 to 0. Prove that every isometry of $\mathbb{F}_q^n$ is the composition of a translation and an element of $\mathbf{Isom}_0(\mathbb{F}_q^n)$.

(5) Let $\mathbf{P}_n$ be the group of maps of the form

$$\phi : \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (x_1, \dots, x_n) & \longmapsto & (\phi_1(x_1), \dots, \phi_n(x_n)) \end{array} \right. ,$$

where, for all $i \in \{1, \dots, n\}$, the map ϕ_i is a permutation of $\mathbb{F}_q$ which fixes 0.

   (a) Prove that $\mathbf{P}_n$ is a subgroup of $\mathbf{Isom}_0(\mathbb{F}_q^n)$.

   (b) Prove that $\mathbf{Isom}_0(\mathbb{F}_q^n)$ is generated by $\mathbf{P}_n$ and $\mathfrak{S}_n$.

   Indication: Prove that a weight 1 *codeword is sent on a weight* 1 *one and then reason by induction on higher weights.*

   More precisely (same remark about the semi-direct product) that

$$\mathbf{Isom}_0(\mathbb{F}_q^n) = \mathbf{P}_n \rtimes \mathfrak{S}_n,$$

   and describe the corresponding action of $\mathfrak{S}_n$ on $\mathbf{P}_n$.

(6) Give the description of a general Hamming isometry.