EXERCISES N° 3, MDS AND REED–SOLOMON CODES

Exercise 1 (Singleton bound for nonlinear codes). Let $C \subseteq \mathbb{F}_q^n$ be a nonlinear code of minimum distance $d$. Prove that $$|C| \leq q^{n-d+1}.$$ 

Indication: use the restriction to $C$ of the map \[ \mathbb{F}_q^n \rightarrow \mathbb{F}_q^{n-d+1}, \quad x \mapsto (x_d, \ldots, x_n). \]

Exercise 2 (Extended Reed–Solomon Codes). Let $\alpha \overset{\text{def}}{=} (\alpha_1, \ldots, \alpha_q) \in \mathbb{F}_q^n$ 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
\[ \mathbb{F}_q[z]_{<k} \rightarrow \mathbb{F}_q^{q+1}, \quad f \mapsto (f(\alpha_1), \ldots, f(\alpha_q), \text{ev}_{\infty,k-1}(f)). \]

(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 $f$. In particular, it is 0 if and only if $f$ has degree $< k - 1$.

(2) Prove that $\text{ERS}_k(\alpha)$ 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 $\mathcal{I} = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$. Recall that the shortening of $C$ at $\mathcal{I}$ is defined as
\[ \mathcal{S}_\mathcal{I}(C) \overset{\text{def}}{=} \{(c_{i_1}, \ldots, c_{i_r}) \mid c \in C, \text{ such that } \forall i \notin \mathcal{I}, c_i = 0\}. \]

Let $1 \leq r \leq k$, we denote the $r$–th generalised Hamming weight $d_r$ of $C$ as the minimal size of a subset $\mathcal{I} \subseteq \{1, \ldots, n\}$ such that the subcode of words whose support is contained in $\mathcal{I}$ has dimension $r$. That is,
\[ d_r \overset{\text{def}}{=} \min \{|\mathcal{I}| \mid \dim \mathcal{S}_\mathcal{I}(C) = r\}. \]

(1) Prove that $d_1$ is nothing but the minimum distance $d$ of $C$.

(2) Prove that the sequence $d_1, d_2, \ldots, d_k$ is strictly increasing.

(3) Prove that if $C$ is an $[n,k,d]$ Reed-Solomon code, then for all $i \leq k$,
\[ d_i = n - k + i. \]

(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 $\varphi : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ such that
\[ \forall x, y \in \mathbb{F}_q^n, \quad d_H(\varphi(x), \varphi(y)) = d_H(x, y), \]
where $d_H$ denotes the Hamming distance.
(1) Prove that isometries are bijective and that the set $\text{Isom}(\mathbb{F}_q^n)$ 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 $\text{Aut}(\mathbb{F}_q^n)$ be the subgroup of $\text{Isom}(\mathbb{F}_q^n)$ of linear isometries of $\mathbb{F}_q^n$. These isometries are represented by $n \times n$ matrices. Let $D_n$ be the group of invertible diagonal matrices and $S_n$ be the group of permutation matrices.

(a) Prove that $D_n$ and $S_n$ are subgroups of $\text{Aut}(\mathbb{F}_q^n)$.

(b) Prove that $\text{Aut}(\mathbb{F}_q^n)$ is spanned by $D_n$ and $S_n$.

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

$$\text{Aut}(\mathbb{F}_q^n) = D_n \rtimes S_n$$

where the action of $S_n$ on $D_n$ is the action by permutation on the diagonal coefficients.

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

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

is an isometry.

(4) Let $\text{Isom}_0(\mathbb{F}_q^n)$ be the subgroup of $\text{Isom}(\mathbb{F}_q^n)$ 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 $\text{Isom}_0(\mathbb{F}_q^n)$.

(5) Let $P_n$ be the group of maps of the form

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

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

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

(b) Prove that $\text{Isom}_0(\mathbb{F}_q^n)$ is generated by $P_n$ and $S_n$.

*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

$$\text{Isom}_0(\mathbb{F}_q^n) = P_n \rtimes S_n,$$

and describe the corresponding action of $S_n$ on $P_n$.

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