EXERCISES N° 3, MDS AND REED–SOLOMON CODES, WITH SOLUTIONS

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 $\left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ x & \longmapsto & (x_d, \ldots, x_n) \end{array} \right.$.

Exercise 2 (Extended Reed–Solomon Codes)**.** Let $\alpha \stackrel{\text{def}}{=} (\alpha_1, \ldots, \alpha_q) \in \mathbb{F}_q^n$ be such that the α_i's are pairwise distinct. That is, the set of elements of $\mathbb{F}_q$ is $\{\alpha_1, \ldots, \alpha_q\}$. 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

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

(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 $\mathcal{I} = \{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$. Recall that the shortening of C at $\mathcal{I}$ is defined as

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

Let $1 \leqslant r \leqslant k$, we denote the r–th generalised Hamming weight d_r of C as the minimal size of a subset $\mathcal{I} \subseteq \{1, \ldots, n\}$ 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 $d_1, d_2, \ldots, d_k$ 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
$$\phi : \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (x_1, \ldots, x_n) & \longmapsto & (\phi_1(x_1), \ldots, \phi_n(x_n)) \end{array} \right. ,$$
   where, for all $i \in \{1, \ldots, n\}$, 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.

Solution to Exercise 1 Let φ be the map

$$\varphi : \left\{ \begin{array}{ccc} C & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ x & \longmapsto & (x_d, \ldots, x_n) \end{array} \right. .$$

We will prove that ϕ is injective. Be careful that, since C is nonlinear, one cannot use any linearity argument. We need to prove injectivity by by classical arguments: let $c, c' \in C$ such that $\varphi(c) = \varphi(c')$. Then, by definition of φ, we get

$$d_H(c, c') \leqslant d - 1.$$

Hence, by definition of the minimum distance for nonlinear codes[1], we get $c = c'$ and hence φ is injective, which proves that

$$|C| \leqslant |\mathbb{F}_q^{n-d+1}| = q^{n-d+1}.$$

Solution to Exercise 2

(1) Let $f \in \mathbb{F}_q[z]_{<k}$:

$$f(z) = f_0 + f_1 z + \cdots + f_{k-1} z^k,$$

with $f_0, f_1, \ldots f_{k-1} \in \mathbb{F}_q$ (possibly zero). Then, a brief computation gives

$$z^{k-1} f(1/z) = f_{k-1} + f_{k-2} z + \cdots + f_1 z^{k-2} + f_0 z^{k-1}$$

which yields the result.

(2) Such a code has length $n \stackrel{\text{def}}{=} q + 1$. We need to compute the minimum distance of this code. Let $c \in \mathbf{ERS}_k(\alpha) \setminus \{0\}$, if c corresponds to a polynomial of degree $k-1$, then, since it has at most $k-1$ distinct roots among the elements of $\mathbb{F}_q$ and that, from the previous question, $ev_{\infty,k-1}(f) \neq 0$, we get

$$n - w_H(c) \leqslant k - 1 \implies w_H(c) \geqslant n - k + 1.$$

Now, if $\deg f \leqslant k-2$, then it has less than $k-2$ distinct roots and vanishes at infinity, which yields also

$$n - w_H(c) \leqslant k - 1 \implies w_H(c) \geqslant n - k + 1.$$

Thus, the minimum distance of C is bounded below by $n-k+1$ and this lower bound is reached thanks to the Singleton bound. Thus, ERS codes are MDS.

(3) We will prove that $\mathbf{ERS}_{q+1-k}(\alpha) = \mathbf{ERS}_k(\alpha)^\perp$. Notice that the sum of the dimensions of these codes equals their length, hence to prove their duality, it is enough to prove that one is included in the other's dual, or equivalently to prove that any element of $\mathbf{ERS}_k(\alpha)$ is orthogonal to any element of $\mathbf{ERS}_{q+1-k}(\alpha)$.

The code $\mathbf{RS}_k(\alpha)$ is a full support Reed-Solomon code and it is known that its dual is $\mathbf{RS}_{q-k}(\alpha)$ (a complete proof of that fact is given after the present exercise's solution). From the duality for Reed–Solomon codes, one gets easily the orthogonality of $c \in \mathbf{ERS}_k(\alpha)$ and $c' \in \mathbf{ERS}_{q+1-k}(\alpha)$, corresponding respectively to polynomials f and g, then

$$\langle c, c' \rangle = \left(\sum_{i=1}^{q} f(\alpha_i) g(\alpha_i) \right) + ev_{\infty,k-1}(f) ev_{\infty,q-k}(g).$$

[1] $d \stackrel{\text{def}}{=} \min_{x \neq y \in C} \{d_H(x, y)\}$.

Notice that the term between parentheses is the scalar product of two words in $\mathbf{RS}_k(\alpha)$ and $\mathbf{RS}_{q+1-k}(\alpha)$, which by duality is zero if either $c \in \mathbf{RS}_{k-1}(\alpha)$ or $c' \in \mathbf{RS}_{q-k}(\alpha)$. The second term (the product of evaluations at infinity) also vanishes, by definition of evaluation at infinity if either $\deg f < k-1$ or $\deg g < q+1-k$, that is if either $c \in \mathbf{RS}_{k-1}(\alpha)$ or $c' \in \mathbf{RS}_{q-k}(\alpha)$. Thus, we have

$$\langle c, c' \rangle = 0, \qquad \text{if } c \in \mathbf{RS}_{k-1}(\alpha) \text{ or } c' \in \mathbf{RS}_{q-k}(\alpha).$$

By linearity, to conclude we only have to prove the orthogonality of c, c' corresponding respectively to the polynomials z^{k-1} and z^{q-k}. Indeed, every codeword of $\mathbf{RS}_k(\alpha)$ is a linear combination of c and a codeword of $\mathbf{RS}_{k-1}(\alpha)$ and every codeword of $\mathbf{RS}_{q+1-k}(\alpha)$ is a linear combination of c' and a word of $\mathbf{RS}_{q-k}(\alpha)$ and one could conclude by the bilinearity of the scalar product. Thus let us prove that $\langle c, c' \rangle = 0$.

$$\langle c, c' \rangle = \left(\sum_{i=1}^{q} \alpha_i^{k-1} \alpha_i^{q-k} \right) + ev_{\infty,k-1}(z^{k-1}) ev_{\infty,q-k}(z^{q-k}) \tag{1}$$

$$= \left(\sum_{i=1}^{q} \alpha_i^{q-1} \right) + 1 \tag{2}$$

$$= \left(\sum_{\alpha \in \mathbb{F}_q} \alpha^{q-1} \right). \tag{3}$$

Finally, recall that

$$\forall \alpha \in \mathbb{F}_q,\ \alpha^{q-1} = \begin{cases} 1 & \text{if} \quad \alpha \neq 0 \\ 0 & \text{if} \quad \alpha = 0 \end{cases}$$

Thus,

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^{q-1} = q - 1 = -1$$

since $q \equiv 0$ modulo the characteristic of the field. Back to (3), we get

$$\langle c, c' \rangle = -1 + 1 = 0.$$

This concludes the proof.

Solution to exercise 3

(1) Let c be a minimum weight codeword. Then, its support has d elements $i_1, \ldots, i_d$. If there exists another codeword $c' \in C$ non collinear to c and supported by $i_1, \ldots, i_d$, then, by eliminiation, one could construct a linear combination of c, c' which is supported by $i_2, \ldots, i_d$. This would give a nonzero codeword of C of weight smaller than the minimum distance, which contradicts the existence of c'. Therefore, the subspace of C of vectors supported by $i_1, \ldots, i_d$ has dimension 1 and is spanned by c. Thus, $d_1 \leqslant d$. Conversely, by definition of the minimum distance, for every subset $\mathcal{I} \subseteq \{1, \ldots, n\}$ with $|\mathcal{I}| < d$, the subspace of codewords of C supported by $\mathcal{I}$ is $\{0\}$, thus $d_1 \geqslant d$, which concludes the proof.

(2) We prove that for all $i \geqslant 1$, $d_i < d_{i+1}$. Let $\mathcal{I} \subseteq \{1, \ldots, n\}$ with $|\mathcal{I}| = i+1$ and such that $\mathcal{S}_{\mathcal{I}}(C)$ has dimension $i+1$. Then, by Gaussian elimination, there exists a subcode of $\mathcal{S}_{\mathcal{I}}(C)$ supported by $\mathcal{I}' \subsetneq \mathcal{I}$ and of dimension i. Thus,

$$d_i \leqslant |\mathcal{I}'| < d_{i+1}.$$

(3) Let $C = RS_k(\alpha)$ for some support $\alpha = (\alpha_1, \ldots, \alpha_n)$, where the α_i's are pairwise distinct elements of $\mathbb{F}_q$. Since the minimum distance of an RS code is $n-k+1$, the result is true for $i = 1$. By induction, assume the result to be true for $i \geqslant 1$, that is $d_i = n-k+i$. From the previous question, since the sequence (d_i) is strictly increasing then $d_{i+1} \geqslant n-k+i+1$. Now, consider a set $\mathcal{I} = \{i_1, \ldots, i_{n-k+i+1}\} \subseteq \{1, \ldots, n\}$ and consider $\mathcal{S}_{\mathcal{I}}(C)$, which corresponds to the evaluation of the space polynomials vanishing at α_j for $j \in \{1, \ldots, n\} \setminus \mathcal{I}$, that is, the polynomials of the form

$$\left(\prod_{i \notin \mathcal{I}} (z - \alpha_i)\right) g(z)$$

with $\deg g < k - (n - |\mathcal{I}|)$. The corresponding space has dimension

$$k - (n - |\mathcal{I}|) = i + 1.$$

Therefore, $d_{i+1} = n - k + i + 1$.

(4) Let C be an MDS code of dimension k. By the previous questions, we have $d_1 = d = n - k + 1$. Since the sequence of generalised weights, is strictly increasing, then we have for all i,

$$d_i \geqslant n - k + i. \tag{4}$$

Finally, let $\mathcal{I} \subset \{1, \ldots, n\}$ with $|\mathcal{I}| = n - k + i$. By Gaussian elimination, the space of codewords supported by $\mathcal{I}$ has dimension at least

$$k - (n - |\mathcal{I}|) = k - (n - (n - k + i)) = i.$$

which entails $d_i \leqslant |\mathcal{I}|$ and hence, thanks to (4), we get the result.

Solution to Exercise 4

(1) Let $x, y \in \mathbb{F}_q^n$ such that $\varphi(x) = \varphi(y)$, then $d_H(\varphi(x), \varphi(y)) = 0$ and hence $d_H(x, y) = 0$, which entails $x = y$. Thus, φ is injective and since $\mathbb{F}_q^n$ is a finite set, the map is surjective too. Thus, it is bijective.

To prove that isometries form a group with respect to the composition, we need that the composition of isometries is an isometry and that the inverse map of an isometry is an isometry too. Both assertions are direct consequences of the definition of an isometry.

(2) (a) Notice that a linear isometry is a linear map which preserves the distance, which for linear maps is equivalent with preserving the Hamming weight. It is elementary to prove that the elements of the groups $\mathbf{D}_n$ and $\mathfrak{S}_n$ preserve the weight.

(b) Such an automorphism sends 0 to 0, then let $e_1, \ldots, e_n$ be the canonical basis of $\mathbb{F}_q^n$, these words have weight 1 and hence their images by φ also have weight 1. Moreover, since for all $i \neq j$, $d_H(e_i, e_j) = 2$, then

$$d_H(\varphi(e_i), \varphi(e_j)) = 2. \tag{5}$$

Therefore, one sees easily that for all $i \in \{1, \ldots, n\}$, there exists $\sigma(i) \in \{1, \ldots, n\}$ and $\lambda_i \in \mathbb{F}_q^\times$ such that

$$\varphi(e_i) = \lambda_i e_{\sigma(i)}$$

and, from (5), the $\sigma(i)$'s are pairwise distinct. Thus, the map σ is a permutation in $\mathfrak{S}_n$. Now, let D be the linear map represented by the invertible diagonal matrix $Diag(\lambda_1, \ldots, \lambda_n)$, then the map $D \circ \sigma$ coincides with φ on the canonical basis. Since they are both linear and coincide on a basis, then they are equal. Thus, every element of $\mathbf{Aut}(\mathbb{F}_q^n)$ is a composition of an element of $\mathbf{D}_n$ and an element of $\mathfrak{S}_n$.
To conclude (if you like semi-direct products), one can check that $\mathbf{D}_n$ is a normal subgroup of $\mathbf{Aut}(\mathbb{F}_q^n)$ (it suffices to check that the conjugation of a diagonal matrix by a permutation matrix is diagonal) there is a short exact sequence

$$\{1\} \longrightarrow \mathbf{D}_n \longrightarrow \mathbf{Aut}(\mathbb{F}_q^n) \longrightarrow \mathfrak{S}_n \longrightarrow \{1\}$$

This sequence splits: a section $\mathfrak{S}_n \to \mathbf{Aut}(\mathbb{F}_q^n)$ is given by the natural injection. Thus the automorphism group is a semi-direct product of the left and right operands of the short exact sequence.

(3) Let $x, y \in \mathbb{F}_q$. Then

$$d_H(x + u, y + u) = w_H(x + u - (y + u)) = w_H(x, y) = d_H(x, y).$$

(4) Given an isometry φ, then $t_{-\varphi(0)} \circ \varphi$ fixes 0. Thus

$$\varphi = t_{\varphi(0)} \circ (t_{-\varphi(0)} \circ \varphi)$$

where $t_{-\varphi(0)} \circ \varphi \in \mathbf{Isom}_0(\mathbb{F}_q^n)$.

(5) (a) Let $\phi \in \mathbf{P}_n$. One sees easily that ϕ fixes 0. Then, let $x, y \in \mathbb{F}_q^n$. The distance $d_H(\phi(x), \phi(y))$ is the number of positions i at which $\phi_i(x_i) \neq phi_i(y_i)$. Since the ϕ_i's are permutations, these positions are the positions at which $x_i \neq y_i$ whose number is $d_H(x, y)$. Thus, ϕ is an isometry fixing 0.

(b) Let $\varphi \in \mathbf{Isom}_0(\mathbb{F}_q^n)$. Then, as in the linear case, we consider the vectors $e_1, \ldots, e_n$ of the canonical basis. Since their distance to 0 is 1 and the distance between two distinct such words is 2, then so does their images. Thus, as in the linear case, there exists a permutation $\sigma \in \mathfrak{S}_n$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q^\times$ such that

$$\forall i \in \{1, \ldots, n\},\ \varphi(e_i) = \lambda_i e_{\sigma(i)}.$$

Moreover, for $i \in \{1, \ldots, n\}$, and for $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$,

$$d_H(e_i, \alpha e_i) = 1,$$

thus, $\varphi(\alpha e_i)$ has distance 1 with $\varphi(e_i) = \lambda_i e_{\sigma(i)}$. By this manner we obtain the existence of a permutation ϕ_i of $\mathbb{F}_q$ fixing 0 and such that

$$\forall \alpha \in \mathbb{F}_q,\ \varphi(\alpha e_i) = \phi_i(\alpha) e_{\sigma(i)}.$$

Set $\phi \stackrel{\text{def}}{=} (\phi_1, \ldots, \phi_n) \in \mathbf{P}_n$. Then, φ and $\phi \circ \sigma$ coincide on the set of words of weight 0 and 1. To prove their equality, we prove that φ and $\phi \circ \sigma$ on the set of words of weight k for all k. For that, we reason by induction on k. The result holds for $k = 0, 1$ (it is what we just proved). Let $k \geqslant 1$, assume the

result to be true for all weights $\leqslant k$. Let $x \in \mathbb{F}_q^n$ of weight $k+1$. Its support is $\{i_1, \ldots, i_{k+1}\} \subseteq \{1, \ldots, n\}$ and its decomposition in the canonical basis is:

$$x = x_{i_1} e_{i_1} + \cdots + x_{i_{k+1}} e_{i_{k+1}}$$

Set $y \stackrel{\text{def}}{=} x_{i_1} e_{i_1} + \cdots + x_{i_k} e_{i_k}$ such that

$$x = y + x_{i_{k+1}} e_{i_{k+1}}.$$

We have

(i) $d_H(x, 0) = k+1$;
(ii) $d_H(x, y) = 1$;
(iii) $d_H(x, x_{i_{k+1}} e_{i_{k+1}}) = k$;
(iv) $d_H(y, x_{i_{k+1}} e_{i_{k+1}}) = k+1$.

Using the above distances and the induction hypothesis, we prove that

(I) $d_H(\varphi(x), 0) = k+1$;
(II) $d_H(\varphi(x), \phi\sigma(y)) = 1$;
(III) $d_H(\varphi(x), \phi_{i_{k+1}}(x_{i_{k+1}}) e_{\sigma(i_{k+1})}) = k$;
(IV) $d_H(\phi\sigma(y), \phi_{i_{k+1}}(x_{i_{k+1}}) e_{\sigma(i_{k+1})}) = k+1$.

And one checks easily, that the only possible value for $\varphi(x) = \phi\sigma(x)$.
Thus every element of $\mathbf{Isom}_0(\mathbb{F}_q^n)$ can be written as the composition $\phi\sigma$ with $\phi \in \mathbf{P}_n$ and $\sigma \in \mathfrak{S}_n$. The semi-direct product is obtained by proving that $\mathbf{P}_n$ is a normal subgroup of $\mathbf{Isom}_0(\mathbb{F}_q^n)$. Then the short exact sequence:

$$\{1\} \longrightarrow \mathbf{P}_n \longrightarrow \mathbf{Isom}_0(\mathbb{F}_q^n) \longrightarrow \mathfrak{S}_n \longrightarrow \{1\}$$

splits, using the same section as in the linear case and this yields the structure of semi-direct product.

(6) Every isometry can be written as the composition $t \circ \phi \circ \sigma$ with t a translation, $\phi \in \mathbf{P}_n$ and $\sigma \in \mathfrak{S}_n$.