EXERCISES N° 2, DUALITY, WITH SOLUTIONS

Exercise 1. Let $C \subset \mathbb{F}_q^n$ be a code. Let $\mathcal{I} \subseteq \{1, \dots, n\}$. We define the following codes constructed from C:

- The punctured code on $\mathcal{I}$ is defined as:
$$\mathcal{P}_{\mathcal{I}}(C) := \{ (c_i)_{i \in \mathcal{I}} \mid c \in C, \} \subseteq \mathbb{F}_q^{|\mathcal{I}|}.$$
Roughly speaking, it is the set of codewords of C where the positions out of $\mathcal{I}$ are removed.
- The shortened code on $\mathcal{I}$ is defined as:
$$\mathcal{S}_{\mathcal{I}}(C) := \{ (c_i)_{i \in \mathcal{I}} \mid c \in C, \forall i \notin \mathcal{I}, c_i = 0\} \subseteq \mathbb{F}_q^{|\mathcal{I}|}.$$
It is the set of codewords supported by $\mathcal{I}$ which is punctured at $\mathcal{I}$

Prove that $(\mathcal{P}_{\mathcal{I}}(C))^{\perp} = \mathcal{S}_{\mathcal{I}}(C^{\perp})$ and $(\mathcal{S}_{\mathcal{I}}(C))^{\perp} = \mathcal{P}_{\mathcal{I}}(C^{\perp})$

Exercise 2. Let $\mathbb{F}_{q^m}/\mathbb{F}_q$ be an extension of finite fields. Recall that the *trace* of $\mathbb{F}_{q^m}/\mathbb{F}_q$ is defined as:
$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \left\{ \begin{array}{ccc} \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & x + x^q + x^{q^2} + \cdots + x^{q^{m-1}} \end{array} \right. .$$

(1) Prove that this map is an $\mathbb{F}_q$–linear form over $\mathbb{F}_{q^m}$.
(2) Prove that this map is surjective.
Indication: use the fact that the polynomial $X + X^q + \cdots + X^{q^{m-1}}$ cannot have q^m roots.
(3) Prove that the map
$$\left\{ \begin{array}{ccc} \mathbb{F}_{q^m} \times \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q \\ (x, y) & \longmapsto & \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xy) \end{array} \right.$$
is $\mathbb{F}_q$–bilinear, symmetric and non degenerated.
(4) Deduce from the previous question that for all linear form $\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_q$, there exists a unique $a_\varphi \in \mathbb{F}_{q^m}$ such that
$$\forall x \in \mathbb{F}_{q^m},\ \varphi(x) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a_\varphi x).$$
(5) Let $C \subseteq \mathbb{F}_{q^m}^n$, we recall the definitions of subfield subcodes and trace codes:
$$\begin{aligned} C_{|\mathbb{F}_q} &:= C \cap \mathbb{F}_q^n \\ \mathrm{Tr}(C) &:= \left\{ \left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \dots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n) \right) \mid c \in C \right\}. \end{aligned}$$
Prove that we always have $C_{|\mathbb{F}_q} \subseteq \mathrm{Tr}(C)$.
Indication: Because of the surjectivity of $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, there exists $\gamma \in \mathbb{F}_{q^m}$ such that $Tr_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) = 1$.

Exercise 3. $\star$
Prove additive Hilbert's 90 Theorem for finite fields:
$$\forall x \in \mathbb{F}_{q^m},\ \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = 0 \iff \exists a \in \mathbb{F}_{q^m},\ x = a^q - a.$$

Exercise 4. $\star$

The goal of this exercise is to prove Delsarte's Theorem: For all code $C \subseteq \mathbb{F}_{q^m}^n$,

$$\left(C_{|\mathbb{F}_q}\right)^\perp \;=\; \mathrm{Tr}\left(C^\perp\right).$$

(1) Prove inclusion "$\supseteq$".

(2) To prove the converse inclusion, we will prove the equivalent one:

$$\left(\mathrm{Tr}(C^\perp)\right)^\perp \subseteq C_{|\mathbb{F}_q}.$$

For that we assume this inclusion to be wrong and take $y \in \left(\mathrm{Tr}(C^\perp)\right)^\perp \setminus C_{|\mathbb{F}_q}$.

(a) Regarding y as an element of $\mathbb{F}_{q^m}^n$ (instead of $\mathbb{F}_q^n$), prove the existence of $x \in C^\perp$ such that $\langle x, y\rangle_{\mathbb{F}_{q^m}^n} \neq 0$.

(b) Prove the existence of $\gamma \in \mathbb{F}_{q^m}$, such that

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}\left(\gamma\langle x, y\rangle_{\mathbb{F}_{q^m}^n}\right) \neq 0.$$

(c) Prove that $\langle \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma x), y\rangle_{\mathbb{F}_q^n} \neq 0$.

(d) Conclude.

(3) Prove that if C is $[n,k,d]_{q^m}$ then $C_{|\mathbb{F}_q}$ is $[n, \geqslant n - m(n-k), \geqslant d]_q$.

Exercise 5. Let C be the binary Hamming code with parity-check matrix

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(1) Prove that C is $[7,4,3]_2$.

(2) Prove that $(1\ 1\ 1\ 1\ 1\ 1\ 1) \in C$ and deduce that the weight enumerator $P_C^\sharp(x,y)$ is symmetric: $P_C^\sharp(x,y) = P_C^\sharp(y,x)$.

(3) Using McWilliams' identity, compute the polynomials $P_C^\sharp$ and $P_{C^\perp}^\sharp$ without enumerating the codes.

Solution to Exercise 1
From now on, we denote by

$$p_{\mathcal{I}} : \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{|\mathcal{I}|} \\ (c_i)_{i=1}^n & \longmapsto & (c_i)_{i\in\mathcal{I}} \end{array} \right.$$

the puncturing map pat $\mathcal{I}$. Let $c_0 \in \mathcal{S}_{\mathcal{I}}\left(C^{\perp}\right)$. By definition of the shortening, there exists a codeword $c \in C^{\perp}$ such that

(i) $p_{\mathcal{I}}(c) = c_0$;
(ii) for all $i \notin \mathcal{I}$, $c_i = 0$.

Then, for all $c' \in C$, and thanks to (i) and (ii)

$$\langle p_{\mathcal{I}}(c'), c_0\rangle_{\mathbb{F}_q^{|\mathcal{I}|}} = \langle c', c\rangle_{\mathbb{F}_q^n} = 0. \tag{1}$$

where the last equality comes from the fact that $c' \in C$ and $c \in C^{\perp}$. Since, by definition,

$$\mathcal{P}_{\mathcal{I}}(C) = \{p_{\mathcal{I}}(x) \mid x \in C\},$$

then, from (1), we see that c_0 is orthogonal to every word of $\mathcal{P}_{\mathcal{I}}(C)$ and hence

$$\mathcal{S}_{\mathcal{I}}\left(C^{\perp}\right) \subseteq \left(\mathcal{P}_{\mathcal{I}}(C)\right)^{\perp}.$$

Conversely, let $d \in \mathcal{P}_{\mathcal{I}}(C)^{\perp}$. Now, let $d' \in \mathbb{F}_q^n$ be the codeword obtained from d by *extending by zeros*. Namely,

$$\forall i \in \{1, \ldots n\},\ d'_i = \left\{ \begin{array}{lll} 0 & \text{if} & i \notin \mathcal{I} \\ d_i & \text{if} & i \in \mathcal{I} \end{array} \right. .$$

Now, by definition of d', for all $c \in C$, we have

$$\langle c, d'\rangle = \langle p_{\mathcal{I}}(c), d\rangle = 0,$$

where the last equality comes from $p_{\mathcal{I}}(c) \in \mathcal{P}_{\mathcal{I}}(C)$ and $d \in \mathcal{P}_{\mathcal{I}}(C)^{\perp}$. This proves that $d' \in C^{\perp}$ and is supported by $\mathcal{I}$ and hence that $d \in \mathcal{S}_{\mathcal{I}}\left(C^{\perp}\right)$. Therefore, we get the converse inclusion and prove

$$\mathcal{S}_{\mathcal{I}}\left(C^{\perp}\right) = \left(\mathcal{P}_{\mathcal{I}}(C)\right)^{\perp}.$$

Now, replacing C by $C^{\perp}$ and using the bidual identity $\left(C^{\perp}\right)^{\perp} = C$, we get

$$\mathcal{S}_{\mathcal{I}}(C) = \left(\mathcal{P}_{\mathcal{I}}\left(C^{\perp}\right)\right)^{\perp},$$

which, by dualizing yields the other expected identity, namely

$$\left(\mathcal{S}_{\mathcal{I}}(C)\right)^{\perp} = \mathcal{P}_{\mathcal{I}}\left(C^{\perp}\right).$$

Solution to Exercise 2

(1) The Frobenius map

$$\left\{ \begin{array}{ccc} \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & x^q \end{array} \right.$$

is known to be $\mathbb{F}_q$–linear: it is additive

$$\forall x, y \in \mathbb{F}_{q^m},\ (x+y)^q = x^q + y^q.$$

Moreover, since for all $a \in \mathbb{F}_q$, $a^q = a$, this yields

$$\forall a \in \mathbb{F}_q, \forall x \in \mathbb{F}_{q^m},\ (ax)^q = a^q x^q = a x^q.$$

The trace map is a sum of iterates of the Frobenius: it is a sum of compositions of linear maps, thus it is linear. The well-definition, i.e. the fact that it maps $\mathbb{F}_{q^m}$ into $\mathbb{F}_q$ comes from the fact that

$$\forall x \in \mathbb{F}_{q^m},\ x^{q^m} = x$$

and hence,

$$\begin{aligned}\forall x \in \mathbb{F}_{q^m},\ \left(x + x^q + \cdots + x^{q^{m-1}}\right)^q &= x^q + x^{q^2} + \cdots + x^{q^{m-1}} + \underbrace{x^{q^m}}_{=x} \\ &= x + x^q + \cdots + x^{q^{m-1}}.\end{aligned}$$

(2) It is an $\mathbb{F}_q$–linear form $\mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$. In particular its image is contained in a space of dimension 1. For this reason, it is either zero or surjective. We prove it is nonzero: Assume the trace map is zero, then, the polynomial

$$X + X^q + \cdots + X^{q^{m-1}}$$

which is nonzero and has degree q^{m-1} would vanish on the whole space $\mathbb{F}_{q^m}$ and hence would have q^m roots which cannot happen since the number of roots of a nonzero polynomial is upper bounded by its degree.

(3) The symmetry comes from the commutativity of the product in $\mathbb{F}_{q^m}$. The $\mathbb{F}_q$–bilnearity comes from the linearity of the trace map together with the the billinearity if the map $(x, y) \to xy$. Let us prove that it is non degenerated. Let $x \in \mathbb{F}_{q^m} \setminus \{0\}$ be such that

$$\forall y \in \mathbb{F}_{q^m},\ \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xy) = 0 \tag{2}$$

Since x is assumed to be nonzero, then,

$$\forall y \in \mathbb{F}_{q^m},\ \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(y) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xx^{-1}y) = 0,$$

where the last equality is a consequence of (2). This contradicts the fact that the trace is a nonzero map.

(4) It is a classical result of duality. In a finite dimensional vector space V over a field k, every non degenerated symmetric billinear map φ, induces an isomorphism

$$\left\{\begin{array}{ccc} V & \longrightarrow & \mathrm{Hom}_k(V, k) \\ a & \longmapsto & \varphi(a, \cdot) \end{array}\right. .$$

(5) By the surjectivity of the trace map, there exists $\gamma \in \mathbb{F}_{q^m}$ such that $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) = 1$. Now, let $c \in C_{|\mathbb{F}_q}$, then, one proves easily that

$$\begin{aligned}\mathrm{Tr}(\gamma c) &= (\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma c_1), \ldots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma c_n)) \\ &= (\mathrm{Tr}(\gamma)c_1, \ldots, \mathrm{Tr}(\gamma)c_n) \\ &= (c_1, \ldots, c_n).\end{aligned}$$

Indeed, by definition of $C_{|\mathbb{F}_q}$, the c_i's are in $\mathbb{F}_q$ and hence $\forall i, \mathrm{Tr}(\gamma c_i) = \mathrm{Tr}(\gamma)c_i$ by the $\mathbb{F}_q$–linearity of the trace map. Therefore, since $c = \mathrm{Tr}(\gamma c)$ and since $\gamma c \in C$, we get $c \in \mathrm{Tr}(C)$ and hence $C_{|\mathbb{F}_q} \subseteq \mathrm{Tr}(C)$.

Solution to Exercise 3

First, let us prove ($\Longleftarrow$). Let ϕ be the map

$$\phi : \left\{ \begin{array}{ccc} \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^m} \\ a & \longmapsto & a^q - a \end{array} \right.$$

The maps ϕ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ are $\mathbb{F}_q$–linear (the linearity of the trace is proved in Exercise 2 and that of ϕ can be proved by the very same manner). To prove the result, we need to prove that $\mathrm{Im}\phi = \ker \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$.

Let $x \in \mathrm{Im}\phi$, by definition, there exists $a \in \mathbb{F}_{q^m}$ such that $x = a^q - a$. Notice first that,

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a^q) &= a^q + a^{q^2} + \cdots + a^{q^{m-1}} + \underbrace{a^{q^m}}_{=a} \\ &= \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a). \end{aligned}$$

Thus, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a^q - a) = \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a^q) - \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = 0$. This proves that

$$\mathrm{Im}(\phi) \subseteq \ker \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \tag{3}$$

We will prove the converse inclusion by proving that both spaces have the same dimension. The kernel of ϕ is the space of elements $a \in \mathbb{F}_{q^m}$ such that $a^q = a$ which is nothing but $\mathbb{F}_q$. Therefore, the $\mathbb{F}_q$–dimension of the kernel of ϕ is 1. Since ϕ is defined on $\mathbb{F}_{q^m}$ which has $\mathbb{F}_q$–dimension m, then, from the rank–nullity theorem *théorème du rang*),

$$\dim_{\mathbb{F}_q} \mathrm{Im}\phi = m - 1. \tag{4}$$

Since, from Exercise 2 the trace map $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \to \mathbb{F}_q$ is a nonzero $\mathbb{F}_q$–linear form, its kernel has $\mathbb{F}_q$–dimension $m - 1$. Then, putting this last fact together with (3) and (4), we get the equality

$$\mathrm{Im}\phi = \ker \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q},$$

which yields the result.

Solution to Exercise 4

(1) Let $c \in C^\perp$ and $d \in C_{|\mathbb{F}_q}$. Then,

$$\langle \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c), d\rangle = \sum_{i=1}^{n} \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_i) d_i \qquad = \sum_{i=1}^{n} \left(\sum_{j=0}^{m-1} c_i^{q^j} \right) d_i \tag{5}$$

$$= \sum_{j=0}^{m-1} \sum_{i=1}^{n} c_i^{q^j} d_i \tag{6}$$

Then, by definition of $C_{|\mathbb{F}_q}$, for all i, we have $d_i \in \mathbb{F}_q$ using this fact together with the additivity of the Frobenius, se get:

$$\langle \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c), d\rangle = \sum_{j=0}^{m-1} \sum_{i=1}^{n} (c_i d_i)^{q^j} \tag{7}$$

$$= \sum_{j=0}^{m-1} \left(\sum_{i=1}^{n} (c_i d_i) \right)^{q^j} \tag{8}$$

$$= \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \left(\langle c, d\rangle \right) = 0. \tag{9}$$

Indeed, by assumption $c \in C^\perp$ and $d \in C_{|\mathbb{F}_q} \subset C$ and hence $\langle c, d\rangle = 0$. This proves

$$\mathrm{Tr}(C^\perp) \subseteq (C_{|\mathbb{F}_q})^\perp.$$

(2) (a) Assume that for all $x \in C^\perp$ we have $\langle x, y\rangle = 0$. Then, this entails that $y \in C$ and since by assumption $y \in \mathbb{F}_q^n$, then $y \in C_{|\mathbb{F}_q}$ which yields a contradiction. This proves the existence of $x \in C^\perp$ such that $\langle x, y\rangle \neq 0$.

(b) This is a direct consequence of Exercise 2 Question 3: since the bilinear form $(x, y) \to \mathrm{Tr}(xy)$ is non degenerate, such a γ exists.

(c)

$$\langle \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma x), y\rangle = \sum_{i=1}^{n} \mathrm{Tr}(\gamma x_i) y_i$$

and, since y has its entries in $\mathbb{F}_q$, this yields

$$\begin{aligned}\langle \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma x), y\rangle &= \sum_{i=1}^{n} \mathrm{Tr}(\gamma x_i y_i) \\ &= \mathrm{Tr}\left(\sum_{i=1}^{n} \gamma x_i y_i\right) \\ &= \mathrm{Tr}(\gamma \langle x, y\rangle).\end{aligned}$$

Since $\mathrm{Tr}(\gamma\langle x, y\rangle)$ has been proved to be nonzero, we get the result.

(d) We proved that $\langle \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma x), y\rangle \neq 0$, thus, $y \notin \mathrm{Tr}(C^\perp)^\perp$ which yields a contradiction.

(3) Regarded as an $\mathbb{F}_{q^m}$–vector space $C^\perp$ has dimension $n - k$, while regarded as an $\mathbb{F}_q$–vector space it has dimension $m(n - k)$. Thus, its image by the $\mathbb{F}_q$–linear trace map has dimension at least $m(n - k)$ (with equality if and only if the restriction of the trace to $C^\perp$ is injective). Therefore,

$$\dim_{\mathbb{F}_q} \mathrm{Tr}(C^\perp) \leqslant m(n-k) \implies \dim_{\mathbb{F}_q} \mathrm{Tr}(C^\perp)^\perp \geqslant n - m(n-k).$$

By Delsarte's Theorem, we get the lower bound on the dimension of $C_{|\mathbb{F}_q}$. For the minimum distance, we just have to notice that we have the inclusion $C_{|\mathbb{F}_q} \subset C$, hence the minimum distance of $C_{\mathbb{F}_q}$ is at least equal to that of C.

Solution to Exercise 5

(1) Consider the rows number $1, 2$ and 4 of the given parity check matrix. The corresponding 3×3 submatrix is the identity matrix and hence the parity check matrix has rank 3. Thus, the code has dimension 4.

For the minimum distance, we use the fact that the minimum distance is the smallest number of linearly linked rows. Notice that the parity check matrix has no zero column and no pair of collinear columns (over $\mathbb{F}_2$, two nonzero vectors are collinear if and only if they are equal!). Thus the minimum distance is larger than or equal to 3. It is equal to 3 since the 3 first columns are linked.

(2) The matrix $\times$ vector product is left to the reader. Since $\mathbf{1} \stackrel{\text{def}}{=} (1, 1, \ldots, 1) \in C$, for all $c \in C$, we have $(\mathbf{1} - c) \in C$ and $W_H(\mathbf{1} - c) = 7 - w_H(c)$. This gives the symmetry: the sets of codewords of weight x and $7 - x$ have equal cardinalities thanks to the

bijection given by $c \mapsto \mathbf{1} - c$. This yields the symmetry of the homogeneous weight enumerator polynomial.

(3) The code C has one word of weight 0, namely, the zero codeword and no word of weight 1 and 2 since its minimum distance is 3. Since it has 16 codewords and since its homogeneous weight enumerator polynomial is symmetric, we get

$$P_C^{\sharp}(x, y) = y^7 + 7x^3y^4 + 7x^4y^3 + x^7.$$

Then, applying McWilliams' formula, we get

$$P_{C^{\perp}}^{\sharp}(x, y) = 7x^4y^3 + y^7.$$