EXERCISES N° 2, DUALITY

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:
$$C_{|\mathbb{F}_q} := C \cap \mathbb{F}_q^n$$
$$\mathrm{Tr}(C) := \left\{ \left(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \dots, \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n) \right) \mid c \in C \right\}.$$
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 $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \in C$ 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.