EXERCISES N° 2, DUALITY

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

- The punctured code on $I$ is defined as:
  $$\mathcal{P}_I(C) := \{(c_i)_{i \in I} \mid c \in C, c \in \mathbb{F}_q^n\} \subseteq \mathbb{F}_q^{|I|}.$$  
  Roughly speaking, it is the set of codewords of $C$ where the positions out of $I$ are removed.

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

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

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:

$$\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q, \quad x \mapsto x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}.$$  

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

$$\begin{cases}
\mathbb{F}_{q^m} \times \mathbb{F}_{q^m} & \rightarrow & \mathbb{F}_q \\
(x, y) & \mapsto & \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(xy)
\end{cases}$$

is $\mathbb{F}_q$–bilinear, symmetric and non degenerated.
4. Deduce from the previous question that for all linear form $\varphi : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q$, there exists a unique $a_\varphi \in \mathbb{F}_{q^m}$ such that

$$\forall x \in \mathbb{F}_{q^m}, \quad \varphi(x) = \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a_\varphi x).$$
5. Let $C \subseteq \mathbb{F}_{q^m}$, we recall the definitions of subfield subcodes and trace codes:

$$C|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^n$$

$$\text{Tr}(C) := \{(\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_1), \ldots, \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(c_n)) \mid c \in C\}.$$  

Prove that we always have $C|_{\mathbb{F}_q} \subseteq \text{Tr}(C)$.

*Indication: Because of the surjectivity of $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$, there exists $\gamma \in \mathbb{F}_{q^m}$ such that $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\gamma) = 1$.

Exercise 3. ⋆
Prove additive Hilbert’s 90 Theorem for finite fields:

$$\forall x \in \mathbb{F}_{q^m}, \quad \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = 0 \iff \exists a \in \mathbb{F}_{q^m}, \quad x = a^q - a.$$
Exercise 4. ⋆
The goal of this exercise is to prove Delsarte’s Theorem: For all code \( C \subseteq \mathbb{F}_q^n \),
\[
(C_{\mathbb{F}_q})^\perp = \text{Tr}(C^\perp).
\]
(1) Prove inclusion “\( \supseteq \)”. 
(2) To prove the converse inclusion, we will prove the equivalent one:
\[
\left( \text{Tr}(C^\perp) \right)^\perp \subseteq C_{\mathbb{F}_q}.
\]
For that we assume this inclusion to be wrong and take \( y \in \left( \text{Tr}(C^\perp) \right)^\perp \setminus C_{\mathbb{F}_q} \). 
(a) Regarding \( y \) as an element of \( \mathbb{F}_q^m \) (instead of \( \mathbb{F}_q^n \)), prove the existence of \( x \in C^\perp \) such that \( \langle x, y \rangle_{\mathbb{F}_q^m} \neq 0 \). 
(b) Prove the existence of \( \gamma \in \mathbb{F}_q^m \), such that
\[
\text{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q}(\gamma \langle x, y \rangle_{\mathbb{F}_q^m}) \neq 0.
\]
(c) Prove that \( \langle \text{Tr}_{\mathbb{F}_q^m/\mathbb{F}_q}(\gamma x), y \rangle_{\mathbb{F}_q^m} \neq 0 \). 
(d) Conclude.
(3) Prove that if \( C \) is \([n, k, d]_q\) then \( C_{\mathbb{F}_q} \) is \([n, \geq n - m(n - k), \geq d]_q\).

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.