Master CSI 1

Arithmétique 1

Feuille d'exercices n° 7.

1 On définit sur $\mathbb{F}_q^n$ le produit scalaire :

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

On définit le code dual $C^\perp$ d'un code linéaire C par :

$$C^\perp := \{x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ pour tout } y \in C\}.$$

1. Montrez que $C^\perp$ est un code linéaire.
2. Montrez que, si C est cyclique, alors $C^\perp$ l'est aussi.
3. Montrez que, si C est de dimension k, alors $C^\perp$ est de dimension $n-k$.
4. Montrez que $(C^\perp)^\perp = C$

2 Soit C_1 et C_2 deux codes linéaires sur $\mathbb{F}_q$, de paramètres respectifs (n_1, k_1, d_1) et (n_2, k_2, d_2). On définit

$$C_1 \oplus C_2 = \{(x, y) \in \mathbb{F}_q^{n_1} \times \mathbb{F}_q^{n_2} \mid x \in C_1, y \in C_2\}$$

et, si $n_1 = n_2 = n$,

$$C_1 * C_2 = \{(x, x+y) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \mid x \in C_1, y \in C_2\}.$$

1. Montrez que $C_1 \oplus C_2$ est un code linéaire de paramètres $(n_1+n_2, k_1+k_2, \min(d_1, d_2))$.
2. Montrez que $C_1 * C_2$ est un code linéaire de paramètres $(2n, k_1+k_2, \min(2d_1, d_2))$.

3 Soit γ un élément de $\mathbb{F}_{16}$ racine du polynome $1 + X + X^2 + X^3 + X^4$. Soit la matrice

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 \\ 1 & \gamma^2 & \gamma^4 & \gamma & \gamma^3 \end{bmatrix}.$$

1. Montrer que G est la matrice génératrice d'un code cyclique C sur $\mathbb{F}_{16}$.
2. Expliquer pourquoi C est un code de Reed-Solomon. Quelle est sa distance minimale ?
3. Que peut-on dire des racines du polynome $c(X) = c_0 + c_1X + c_2X^2 + c_3X^3 + c_4X^4$ si $[c_0, c_1, c_2, c_3, c_4]$ est un mot du code dual $C^\perp$ de C ?
4. Trouver le polynome générateur de $C^\perp$.
5. En se servant de $(C^\perp)^\perp = C$, trouver le polynome générateur de C.