Master CSI 1 — 2006-2007

Arithmétique 1

Feuille d'exercices n° 6.

Dans tous les exercices, la longueur n des codes cycliques sur $\mathbb{F}_q$ est supposée première à q.

1 Faire la liste des codes cycliques de longueur 9 et de longueur 15 sur $\mathbb{F}_2$, donner une matrice génératrice de chacun d'eux.

2 Soit $f(X)$ un diviseur de $X^n - 1$ dans $\mathbb{F}_q[X]$ et soit C le code cyclique sur $\mathbb{F}_q$ engendré par f. Soit $d = \deg(f)$.

On note x l'image de X dans le quotient $\mathbb{F}_q[X]/(X^n - 1)\mathbb{F}_q[X]$.

1. Montrez que $B := \{f(x), xf(x), \ldots, x^{n-d-1}f(x)\}$ forme une famille libre de C.
2. Soit $P(X) \in \mathbb{F}_q[X]$. En utilisant la division euclidienne de $P(X)f(X)$ par $X^n - 1$, montrez que $P(x)f(x)$ est combinaison linéaire des éléments de B.
3. Conclure que B est une base de C et que C est de dimension $n - d$.
4. Écrire la matrice $(n - d) \times n$ dont les lignes sont les éléments de B vus dans $\mathbb{F}_q^n$.

3 Tous les codes de cet exercice sont cycliques, de longueur n sur $\mathbb{F}_q$.

1. Montrez que le code cyclique engendré par $1 + X + X^2 + \cdots + X^{n-1}$ est le code $C = \{(a, \ldots, a) : a \in \mathbb{F}_q\}$. Quelle est sa dimension ?
2. Montrez que le code cyclique engendré par $X - 1$ est le code $C = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n : \sum_{i=1}^n x_i = 0\}$. Quelle est sa dimension ?
3. Montrez que, si C_i est engendré par f_i avec f_i diviseur de $X^n - 1$, alors :
   (a) $C_1 \subset C_2 \iff f_2$ divise f_1
   (b) $C_1 + C_2$ est engendré par $\gcd(f_1, f_2)$
   (c) $C_1 \cap C_2$ est engendré par $\mathrm{ppcm}(f_1, f_2)$

4 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 $(C^\perp)^\perp = C$
5. Montrez que les codes des questions 1 et 2 de l'exercice 3 sont duaux l'un de l'autre.
6. Reprendre la liste des codes de l'exo 1 et déterminez les paires $(C, C^\perp)$.
7. En observant les résultats de la question précédente, posez une conjecture sur l'expression du polynôme générateur de $C^\perp$ en fonction de celui de C. Et démontrez-la !