Université de Bordeaux

Master 1 CSI
4TCY703U - Arithmétique
Feuille 6

Exercice 1. Soit K un corps fini. Soient C_1 et C_2 deux codes K-linéaires de paramètres respectifs (n, k_1, d_1) et (n, k_2, d_2). On pose $C = \{(c_1, c_2 - c_1)\,;\, c_1 \in C_1 \text{ et } c_2 \in C_2\}$.
(1) Quelles sont la longueur et la dimension du code linéaire C ?
(2) Montrer que la distance minimale de C est $\min(2d_1, d_2)$.

Exercice 2. Soient K un corps fini, $n \in \mathbf{N}_{\geqslant 1}$ et $a \in K^\times$. Notons C le code (linéaire) de longueur n défini par $C = \{(c, ac, \dots, a^{n-1}c)\,;\, c \in K\}$.
(1) Quels sont les paramètres de C ?
(2) À quelle condition (sur n et a) le code C est-il cyclique ?

Exercice 3. Soient K un corps fini et $n \in \mathbf{N}_{\geqslant 2}$. On pose $C = \{(c_1, \dots, c_n) \in K^n\,;\, c_1 + \cdots + c_n = 0\}$.
(1) Déterminer les paramètres du code linéaire C.
(2) Vérifier que C est un code cyclique et trouver son polynôme générateur.

Exercice 4. Notons C le code $\mathbf{F}_2$-linéaire de matrice de contrôle

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

(1) Déterminer les paramètres de C.
(2) Trouver le mot de C le plus proche de $(0, 1, 1, 0, 0, 1, 0, 0)$.

Exercice 5. Prouver qu'il n'existe pas de code $\mathbf{F}_3$-linéaire de paramètres $(5, 2, 4)$.

Exercice 6. Désignons par C l'ensemble des $(c_0, \dots, c_{14}) \in \mathbf{F}_2^{15}$ tels que $c_{i+4} = c_{i+3} + c_i$ pour tout $i \in \{0, \dots, 10\}$.
(1) Quelle est la dimension du code linéaire C ?
(2) Considérons le mot $(c_0, \dots, c_{14}) \in C$ tel que $(c_0, c_1, c_2, c_3) = (1, 0, 0, 0)$. Calculer c_i pour tout $i \leqslant 14$.
(3) Démontrer que C est un code cyclique.
(4) Quelle est la distance minimale de C ?

Exercice 7. Soient K un corps fini de caractéristique p et n un entier naturel tel que p ne divise pas n.
(1) Soit C un code cyclique sur K de longueur n. Montrer qu'il existe un unique $e \in C$ tel que $e.c = c$ pour tout $c \in C$ (*indication :* utiliser une relation de Bézout entre le polynôme générateur $P(X)$ de C et $(X^n - 1)/P(X)$).
Le mot e est appelé l'*idempotent* de C. Soient C et C' deux codes cycliques de longueur n d'idempotents respectifs e et e'.
(2) Quel est l'idempotent de $C \cap C'$?
(3) Prouver que l'idempotent de $C + C'$ est $e + e' - e.e'$.