Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Feuille de TD 4

08/03/2024

Le corrigé de certains exercices sera disponible à l'adresse suivante :

`https://lvzl.fr/teaching/2023-24/ca.html`

$(\star)$ exercice fondamental $(\star\star)$ pour s'entraîner $(\star\star\star)$ pour aller plus loin 💻 sur machine

Exercice 1. $(\star)$ Application de la borne BCH.

Question 1.– Donner une borne inférieure sur la distance minimale des codes suivants.

1. Le code cyclique binaire de longueur $n = 31$, dont l'ensemble de définition est la réunion des classes cyclotomiques de représentants 1, 3 et 5.
2. Le code cyclique sur $\mathbb{F}_3$ de longueur $n = 8$, dont l'ensemble de définition est la réunion des classes cyclotomiques de représentants 0, 1 et 5.

Question 2.– Donner une borne inférieure sur la distance minimale des codes suivants.

1. Le code cyclique binaire de longueur $n = 15$ et de polynôme générateur
$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1\,.$$
Indication : $\alpha \in \mathbb{F}_{16}$ telle que $\alpha^4 = \alpha + 1$ est une racine primitive n-ème de l'unité.
2. Le code cyclique sur $\mathbb{F}_5$ de longueur $n = 12$ et de polynôme générateur
$$g(x) = x^4 + 2x^3 + 2x^2 - x - 1$$
Indication : $\alpha \in \mathbb{F}_{25}$ tel que $\alpha^2 = 2\alpha + 1$ est une racine primitive n-ème de l'unité.

Exercice 2. $(\star)$ Construction de codes BCH.

Question 1.– Donner le polynôme générateur des codes BCH suivants. On pourra réutiliser des calculs faits précédemment en cours ou en TD.

1. Un code BCH au sens strict, binaire, de longueur $n = 15$ et de distance construite $\delta = 4$.
2. Un code BCH sur $\mathbb{F}_3$, de longueur $n = 13$, de distance construite $\delta = 5$ avec comme premier zéro $b = 0$.

Question 2.– Que donne la borne BCH pour les deux codes construits ci-dessus ?

Exercice 3. $(\star\star)$ Matrice de parité de codes BCH.

Question 1.– Donner une matrice de parité de rang maximal du code BCH au sens strict sur $\mathbb{F}_3$, de longueur 8 et de distance construite 4.

Question 2.– Donner une matrice de parité de rang maximal du code BCH au sens strict sur $\mathbb{F}_7$, de longueur 6 et de distance construite 3.

Exercice 4. $(\star\star\star)$ Ensemble de définition du dual d'un code cyclique.

Soit $\mathcal{C}$ un code cyclique de longueur n sur $\mathbb{F}_q$, défini par un polynôme générateur $g(x)$. On rappelle que, pour un choix de α une racine primitive n-ème de l'unité, l'**ensemble de définition** de $\mathcal{C}$ est

$$I = \left\{ i \in \{0, \ldots, n-1\} \mid g(\alpha^i) = 0 \right\}.$$

Question 1.– Rappeler le lien entre le polynôme générateur d'un code cyclique et celui de son dual.

Question 2.– Démontrer que $I' = \left\{ (-i) \mod n \mid i \in \{0, \ldots, n-1\} \setminus I \right\}$ est l'ensemble de définition de $\mathcal{C}^\perp$, pour le même choix de α.

Question 3.– Application : donner une borne inférieure sur la distance minimale de $\mathcal{C}^\perp$, où $\mathcal{C}$ est le code BCH au sens strict, binaire, de longueur $= 2^m - 1$ et de distance construite 2.