Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Feuille de TD 1

26/01/2024

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. ($\star$) Groupe d'automorphismes du code dual.

Soit $\mathcal{C} \subseteq \mathbb{F}_q^n$ un code linéaire et $\mathrm{PAut}(\mathcal{C})$ son groupe d'automorphismes par permutations. On note $\mathcal{C}^\perp$ de dual de $\mathcal{C}$.

Question 1.– Soient $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ et $\sigma \in \mathfrak{S}_n$ une permutation. Démontrer que

$$\langle \sigma(\boldsymbol{x}), \boldsymbol{y} \rangle = \langle \boldsymbol{x}, \sigma^{-1}(\boldsymbol{y}) \rangle$$

Question 2.– Soit $\boldsymbol{c} \in \mathcal{C}$, $\boldsymbol{h} \in \mathcal{C}^\perp$ et $\sigma \in \mathrm{PAut}(\mathcal{C})$. Démontrer que $\langle \sigma(\boldsymbol{c}), \boldsymbol{h} \rangle = 0$.

Question 3.– En déduire que $\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{PAut}(\mathcal{C}^\perp)$, puis que ces deux groupes sont égaux.

Exercice 2. ($\star$) Reconnaître un code cyclique.

Parmi les codes suivants, lesquels sont cycliques ?

Question 1.– Le code de parité de longueur n sur $\mathbb{F}_q$:

$$\{\boldsymbol{c} \in \mathbb{F}_q^n \mid c_1 + c_2 + \cdots + c_n = 0\}.$$

Question 2.– Le code binaire de matrice génératrice

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Question 3.– Le code binaire de matrice de parité

$$\boldsymbol{H} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Question 4.– Le code binaire de matrice génératrice :

$$\boldsymbol{A} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Question 5.– Le code sur $\mathbb{F}_5$ de matrice génératrice :

$$\boldsymbol{B} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Exercice 3. $(\star)$ Calculs modulo $X^n - 1$.

On note $R_n = \mathbb{F}_q[x]/(x^n - 1)$.

Question 1.– L'élément x est-il inversible dans R_n ? Si oui, calculer son inverse.

Question 2.– L'élément $x - 1$ est-il inversible dans R_n ? Si oui, calculer son inverse.

Question 3.– Dans cette question, on pose $n = 5$ et $q = 2$.

1. Calculer la somme et le produit de $A(x) = x^2 + 1$ et $B(x) = x^3 + x + 1$ dans R_n.
2. Les éléments $A(x)$ et $B(x)$ sont-ils inversibles dans R_n ? Si oui, déterminer leurs inverses.