Université Paris 8 J. Lavauzelle

Master 1 Mathématiques et applications — année 2023–24

Codes algébriques – Solutions feuille de TD 1

26/01/2024

Retrouvez le sujet du TD et d'autres exercices à l'adresse :

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

(⋆) exercice fondamental (⋆⋆) pour s'entraîner (⋆⋆⋆) pour aller plus loin 💻 sur machine

Exercice 1. 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.

Solutions de l'Exercice 1.

Solution Q1. Le calcul du produit scalaire donne :

$$\langle \sigma(\boldsymbol{x}), \boldsymbol{y} \rangle = \sum_{i=1}^{n} \sigma(x_i) y_i = \sum_{i=1}^{n} x_{\sigma^{-1}(i)} y_i = \sum_{j=1}^{n} x_j y_{\sigma(j)} = \sum_{j=1}^{n} x_j \sigma^{-1}(y_j) = \langle \boldsymbol{x}, \sigma^{-1}(\boldsymbol{y}) \rangle .$$

Solution Q2. Comme $\sigma \in \mathrm{PAut}(\mathcal{C})$, pour tout $\boldsymbol{c} \in \mathcal{C}$ on a $\sigma(\boldsymbol{c}) \in \mathcal{C}$. Par conséquent, le produit scalaire entre $\sigma(\boldsymbol{c})$ et $\boldsymbol{h}$ est nul (par définition du code dual).

Solution Q3. Soit $\sigma \in \mathrm{PAut}(\mathcal{C})$ et $\boldsymbol{h} \in \mathcal{C}^\perp$. D'après les questions précédentes, pour tout $\boldsymbol{c} \in \mathcal{C}$, on a

$$\langle \boldsymbol{c}, \sigma^{-1}(\boldsymbol{h}) \rangle = \langle \sigma(\boldsymbol{c}), \boldsymbol{h} \rangle = 0 .$$

Autrement dit, $\sigma^{-1}(\boldsymbol{h})$ est orthogonal à tout mot de $\mathcal{C}$, il appartient donc à $\mathcal{C}^\perp$.

Ceci est vrai pour tout $\boldsymbol{h} \in \mathcal{C}^\perp$, par conséquent σ^{-1} est un automorphisme par permutation de $\mathcal{C}^\perp$. Pour résumer on a donc :

$$\forall \sigma \in \mathrm{PAut}(\mathcal{C}),\ \sigma^{-1} \in \mathrm{PAut}(\mathcal{C}^\perp)$$

Comme $\mathrm{PAut}(\mathcal{C})$ est un groupe, ceci implique que $\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{PAut}(\mathcal{C}^\perp)$.

L'inclusion réciproque se montre en notant que $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. Ainsi on a

$$\mathrm{PAut}(\mathcal{C}^\perp) \subseteq \mathrm{PAut}((\mathcal{C}^\perp)^\perp) = \mathrm{PAut}(\mathcal{C}) .$$

Exercice 2. Distinguer 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 :

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

Solutions de l'Exercice 2.

Solution Q1. Pour cette question, on peut raisonner avec la définition. Soit $\boldsymbol{c}$ un mot du code. Alors, sa permutation cyclique $\boldsymbol{c}' = (c_n, c_1, c_2, \ldots, c_{n-1})$ vérifie :

$$c_n + c_1 + \cdots + c_{n-1} = c_1 + \cdots + c_{n-1} + c_n = 0,$$

donc est aussi un mot de code. Par conséquent, la permutation cyclique est bien automorphisme du code, ce qui est suffisant pour affirmer que le code est cyclique.

Solution Q2. On vérifie que les permutations cycliques des lignes de $\boldsymbol{G}$ sont bien des mots de code. Ici, on peut le faire en observant qu'elles sont des combinaisons linéaires des lignes de $\boldsymbol{G}$ (on verra une autre méthode dans une prochaine question).

1. La permutation cyclique de la première ligne donne la deuxième ligne, elle est donc dans le code.
2. La permutation cyclique de la deuxième ligne vaut $(1, 0, 1, 00, 1, 1)$, ce n'est donc ni la première, ni la troisième ligne de $\boldsymbol{G}$, mais c'est en revanche la somme de ces deux lignes. Donc ce mot est également dans le code.
3. La permutation cyclique de la troisième ligne donne la première ligne, elle est donc aussi dans le code.

Le code engendré par $\boldsymbol{G}$ est donc bien cyclique

Solution Q3. On observe que le code est égal à celui de la question précédente. En effet, si l'on décompose $\boldsymbol{G}$ en deux blocs $(\boldsymbol{I}_3 \mid \boldsymbol{U})$, alots comme $\boldsymbol{H}$ s'écrit bien sous la forme $(-\boldsymbol{U}^\top \mid \boldsymbol{I}_4)$.

Ainsi, le code est cyclique.

Solution Q4. On va montrer que le code n'est pas cyclique. Pour cela, on peut chercher à exhiber un mot dont la permutation cyclique n'appartient pas au code.

Pour montrer qu'un mot n'appartient pas à un code linéaire, on peut montrer qu'il ne satisfait pas les équations de parité du code. Construisons donc une matrice de parité du code ; comme la matrice $\boldsymbol{A}$ est sous forme systématique, c'est immédiat :

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

Puis, cherchons si l'une des permutations de lignes de $\boldsymbol{A}$ ne satisfait pas l'une des deux équations associées aux lignes de $\boldsymbol{M}$. C'est le cas pour la deuxième ligne de $\boldsymbol{A}$, dont la permutation donne $(0,0,1,0,0,0)$ qui ne satisfait l'équation de parité définie par la première ligne de $\boldsymbol{M}$.

Solution Q5. Notons $\mathcal{C}$ le code engendré par $\boldsymbol{B}$. La permutation de la première ligne de $\boldsymbol{B}$ est égale à elle-même, elle reste donc dans $\mathcal{C}$. Pour la deuxième ligne, c'est moins évident.

Une méthode générique consiste ici à calculer une matrice de parité de $\boldsymbol{C}$. On l'obtient par exemple en trouvant une forme systématique pour $\boldsymbol{B}$:

$$\boldsymbol{B}' = \begin{pmatrix} 1 & 0 & 3 & 4 \\ 0 & 1 & 3 & 2 \end{pmatrix}$$

est obtenue en retirant la première ligne à la seconde, puis retirant la seconde ligne à la première.

Une matrice de parité de $\boldsymbol{C}$ est donc

$$\boldsymbol{D} = \begin{pmatrix} -3 & -3 & 1 & 0 \\ -4 & -2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 3 & 0 & 1 \end{pmatrix}.$$

Il reste maintenant à vérifier si le vecteur $\boldsymbol{v} = (3,1,2,4)$, permutation de la deuxième ligne de $\boldsymbol{B}$, satisfait ou non $\boldsymbol{D}\boldsymbol{v}^\top = \boldsymbol{0}$. On a ici :

$$\boldsymbol{D}\boldsymbol{v}^\top = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

donc le code $\boldsymbol{C}$ est cyclique.

Exercice 3. 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.

Solutions de l'Exercice 3.

Solution Q1. On a $x \times x^{n-1} = x^n \equiv 1 \mod (x^n - 1)$, donc x est inversible modulo $x^n - 1$, et son inverse est x^{n-1}.

Solution Q2. On a $x - 1 \times (1 + x + \cdots + x^{n-1}) = x^n - 1 \equiv 0 \mod (x^n - 1)$, donc $x - 1$ n'est pas inversible modulo $x^n - 1$.

Solution Q3.

1. On a
$$A(x) + B(x) \equiv (x^2 + 1) + (x^3 + x + 1) \equiv x^3 + x^2 + x \mod (x^5 + 1)$$
et
$$A(x) \cdot B(x) \equiv (x^2 + 1) \cdot (x^3 + x + 1) \equiv x^5 + x^2 + x + 1 \equiv 1 + x^2 + x + 1 = x^2 + x \mod (x^5 + 1)$$
2. On a $A(x) = x^2 + 1 = (x+1)^2$ et $x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + 1)$. Ces polynômes ne sont donc pas premiers entre eux, par conséquent $A(x)$ n'est pas inversible modulo $x^5 + 1$.

   D'autre part, l'algorithme d'Euclide étendu calculé sur $x^5 + 1$ et $B(x)$ donne la série d'étapes suivantes (faites les calculs !) :
$$x^5 + 1 = (x^2 + 1)B(x) + R(x) \text{ avec } R(x) = x^2 + x$$
$$B(x) = (x + 1)R(x) + 1$$
   donc $B(x)$ est bien inversible modulo $x^5 + 1$ et on obtient son inverse par le calcul du coefficient de Bezout :
$$1 = B(x) + (x + 1)R(x) = (1 + (x + 1)(x^2 + 1))B(x) + (x + 1)(x^5 + 1) = (x^3 + x^2 + x)B(x) + (x + 1)(x^5 + 1)$$
   Ceci implique que l'inverse de $B(x)$ modulo $x^5 + 1$ est $x^3 + x^2 + x$.
