Codes algébriques – Solutions feuille de TD 2

02/02/2024

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

`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. ($\star$) Construire un code cyclique par son générateur.

Question 1.– Donner une matrice génératrice et la dimension du code cyclique de longueur 6 sur $\mathbb{F}_2$ engendré par le polynôme x^2+1.

Question 2.– Donner une matrice génératrice et la dimension du code cyclique de longueur 6 sur $\mathbb{F}_3$ engendré par le polynôme $(x+1)^2(x-1)$.

Solutions de l'Exercice 1.

Solution Q1. Notons $g(x) = x^2+1 \in \mathbb{F}_2[x]$ et considérons le code $\mathcal{C}$ de longueur $n=6$ engendré par $g(x)$. Tout d'abord, on observe que x^2+1 est bien un diviseur de x^6-1. En effet, dans $\mathbb{F}_2[x]$ on a :

$$x^6-1 = x^6+1 = (x^3+1)^2 = (x+1)^2(x^2+x+1)^2 = (x^2+1)\cdot(x^2+x+1)^2\,.$$

Le polynôme $g(x)$ est donc **le** polynôme générateur de $\mathcal{C}$, et d'après le cours :

1. la dimension de $\mathcal{C}$ est donc $n-\deg(g) = 6-2 = 4$
2. une matrice génératrice de $\mathcal{C}$ est donnée par :

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

Solution Q2. Notons $f(x) = (x+1)^2(x-1) \in \mathbb{F}_3[x]$ et considérons le code $\mathcal{C}$ de longueur $n=6$ engendré par $f(x)$. Tout d'abord, on observe que $f(x)$ est bien un diviseur de x^6-1. En effet, dans $\mathbb{F}_2[x]$ on a :

$$(x^6-1) = (x^2-1)^3 = (x-1)^3(x+1)^3 = f(x)\cdot(x-1)^2(x+1)$$

Le polynôme $f(x)$ est donc **le** polynôme générateur de $\mathcal{C}$, et d'après le cours :

1. la dimension de $\mathcal{C}$ est donc $n-\deg(f) = 6-3 = 3$
2. en développant $f(x) = x^3+x^2+2x+2$, on obtient une matrice génératrice de $\mathcal{C}$ donnée par :

$$G = \begin{pmatrix} 2 & 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}$$

Exercice 2. ($\star\star$) Générateurs de codes cycliques.

Donner le polynôme générateur des codes cycliques suivants.

Question 1.– Le code de parité de longueur $n \geq 2$, sur un corps fini $\mathbb{F}_q$ quelconque.

Question 2.– Le code binaire de matrice génératrice

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

Question 3.– 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 4.– Le code associé à l'idéal $\langle x^3 + x^2 \rangle$ de $\mathbb{F}_2[x]/(x^5 - 1)$.

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. Le code parité sur $\mathbb{F}_q$ de longueur n est défini par

$$\mathcal{C} = \left\{ \boldsymbol{c} \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} c_i = 0 \right\}$$

On a déjà vu que c'était un code cyclique. Observons que sa dimension est $n-1$. On cherche donc un générateur $g(x) \in \mathbb{F}_q[x]$ de ce code qui est un diviseur unitaire de $x^n - 1$ de degré $n - (n-1) = 1$.

On sait que

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Le polynôme $x - 1$ semble être un bon candidat. Vérifions-le.

Pour cela, vérifions d'abord que le vecteur associé au polynôme $x - 1$ est bien dans le code. Ce vecteur est :

$$(1, -1, 0, \ldots, 0),$$

et satisfait donc $1 + (-1) + 0 + \cdots + 0 = 0$. Par conséquent le code engendré par $x - 1$ (qui est un code cyclique de dimension $n - 1$) est inclus dans $\mathcal{C}$, lui-même de dimension $n - 1$. Il y a donc égalité, ce qui implique que $g(x) = x - 1$.

Solution Q2. On observe que la matrice $\boldsymbol{A}$ engendre bien un code cyclique, car les permutations cycliques de ses lignes appartiennent toujours au code.

Pour trouver un générateur de $\boldsymbol{A}$, la **méthode générique** est de calculer le pgcd des polyônomes associés aux lignes de $\boldsymbol{A}$. On obtient alors **un** générateur de l'idéal associé au code. Pour obtenir **le** générateur du code, il reste à effectuer un dernier pgcd avec $x^n - 1$. Ici, les deux polynômes sont $a_1(x) = x + x^3 = x(x+1)^2$ et $1 + x^2 = (x+1)^2$. Comme $x^4 - 1 = x^2(x+1)^2$ dans $\mathbb{F}_2[x]$, un calcul rapide donne :

$$\operatorname{pgcd}(1 + x^2, x + x^3, x^4 - 1) = (x+1)^2.$$

Le polynôme générateur du code est donc $(x+1)^2 = 1 + x^2$.

Une **autre manière non-générique** d'obtenir le résultat est de remarquer qu'en réordonnant les lignes de $\boldsymbol{A}$, on obtient une matrice

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

qui est sous la forme standard d'une matrice génératrice de code cyclique :

- la première ligne correspond aux coefficients d'un diviseur unitaire $g(x))1 + x^2$ de $x^n - 1$ (voir calcul ci-dessus),
- les $n - \deg(g(x)) - 1$ lignes suivantes sont des permutation cycliques de la première ligne.

Dans ce cas-là, on sait que $g(x)$ est un générateur du code.

Solution Q3. Comme vu précédemment, on pourrait appliquer ici une méthode générique pour trouver le polynôme générateur du code. Il suffit de calculer le pgcd de $1+x^3+x^4+x^5$, $x+x^4+x^5+x^6$, $x^2+x^3+x^4+x^6$ et x^7-1. Un calcul donne alors le polynôme $1+x+x^2+x^4$.

Ici, soyons plus malins : une autre matrice génératrice du code est :

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

Pour l'obtenir, on a permuté cycliquement les colonnes de la matrice 5 fois, puis on a échangé les lignes. Comme dans la question précédente, on obtient une matrice génératrice de code cyclique dans une forme standard, et la première ligne $g(x) = 1+x+x^2+x^4$ est un diviseur de x^7-1 : en effet, on a $x^7-1 = (1+x)(1+x^2+x^3)(1+x+x^3)$ et $g(x) = (1+x)(1+x^2+x^3)$.

Le polynôme générateur du code cyclique engendré par la matrice $\boldsymbol{G}$ est donc $g(x)$.

Solution Q4. Notons $a(x) = x^3+x^2 \in \mathbb{F}_2[x]$. On cherche le polynome générateur du code cyclique associé à l'idéal $\langle a(x)\rangle$ de $\mathbb{F}_2[x]/\langle x^5-1\rangle$.

Notons d'abord que $a(x)$ ne peut pas être le polynôme générateur de code. En effet, $a(x)$ ne divise pas x^5-1, on a :

$$x^5-1 = (x^2+x+1)a(x) + (x^2+1)$$

Pour obtenir le polynôme générateur du code cyclique, on doit donc calculer le pgcd de $a(x)$ et de x^5-1. Observons que $a(x) = x^2(x+1)$. Comme x est premier avec x^5-1, on a donc :

$$\operatorname{pgcd}(a(x), x^5-1) = x+1$$

Le code cyclique associé à l'idéal $\langle a(x)\rangle$ a donc pour polynôme générateur $x+1$. C'est un code de dimension 4 ; c'est d'ailleurs le code de parité.

Solution Q5. On a vu dans un exercice précédent que ce code était cyclique. Pour calculer son polynôme générateur, on calcule le pgcd des polynômes associés aux deux lignes de la matrice génératrice. Le calcul est un peu fastidieux :

$$1+2x+4x^2+3x^3 = 4\times(1+x+x^2+x^3) + (x^2+4x+3)x^3 + x^2 + x + 1 \quad = (x+2)\times(x^2+4x+3)$$

Ainsi, $\operatorname{pgcd}(1+2x+4x^2+3x^3, 1+x+x^2+x^3) = x^2+4x+3 = (x+1)(x+3)$. Par ailleurs, sur $\mathbb{F}_5$ tous les éléments $z \neq 0$ sont tels que $z^4 = 1$. Ainsi, $x^4-1 = (x+1)(x+2)(x+3)(x+4)$. Le polynôme $(x+1)(x+3)$ est donc aussi un diviseur de x^4-1. On en conclut que c'est le polynôme générateur du code.

Exercice 3. ($\star$) Code dual d'un code cyclique.

Question 1.– Décrire, par un polynôme générateur et par une matrice génératrice, le **dual** du code cyclique de longueur 7 et de polynôme générateur $g(x) = x^3+x+1$ sur $\mathbb{F}_2$.

Question 2.– Décrire, par son polynôme générateur, le **dual** du code cyclique binaire de matrice génératrice

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

Question 3.– On s'intéresse à des codes cycliques de longueur 8 sur $\mathbb{F}_3$.

1. Vérifier que la factorisation en irréductibles de x^8-1 dans $\mathbb{F}_3[x]$ est :
$$x^8-1 = (x-1)\cdot(x+1)\cdot(x^2+1)\cdot(x^2+x-1)\cdot(x^2-x-1).$$
2. Déterminer le **dual** du code cyclique $\mathcal{C}$, de longueur 8 sur $\mathbb{F}_3$, et de polynôme générateur
$$g(x) = 1+x-x^2-x^4-x^5+x^6.$$
3. Démontrer (par un argument simple) que $\mathcal{C}$ est auto-orthogonal c'est-à-dire qu'il vérifie $\mathcal{C} \subseteq \mathcal{C}^\perp$.

Solutions de l'Exercice 3.

Solution Q1. Soit $\mathcal{C}$ le code cyclique binaire de longueur 7 engendré par $g(x) = x^3 + x + 1$. D'après le cours, le polynôme générateur de $\mathcal{C}^\perp$ est

$$g^\perp(x) := x^{7-3}h(x^{-1})$$

où $h(x) = \frac{x^7+1}{g(x)}$. Calculons donc $h(x)$. Un calcul (à faire !) donne

$$x^7 + 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1)$$

puis on obtient

$$g^\perp(x) = x^4 + x^3 + x^2 + 1\,.$$

Le code $\mathcal{C}^\perp$ a donc pour matrice génératrice

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

Solution Q2. On a vu, dans un exercice précédent, que le code engendré par la matrice $\boldsymbol{A}$ était un code cyclique $\mathcal{C}$ de polynôme générateur $x^2 + 1$. On observe que $x^4 - 1 = (x^2 + 1)^2$; ainsi, le dual de $\mathcal{C}$ a pour polynôme générateur le polynôme réciproque de $x^2 + 1$, c'est-à-dire $x^2 + 1$ lui-même.

Remarque. Le code $\mathcal{C}$ est donc égal à son dual, on dit qu'il est auto-dual.

Solution Q3.

1. Il suffit de développer le produit à droite de l'équation à vérifier. Pour rendre le calcul le moins fastidieux possible, on essaie de regrouper les facteurs astucieusement :

   $$(x-1)(x+1)(x^2+1) = (x^2-1)(x^2+1) = x^4 - 1$$

   et

   $$(x^2 + x - 1)(x^2 - x - 1) = (x^2 - 1)^2 - x^2 = x^4 - 2x^2 + 1 - x^2 = x^4 + 1$$

   donc le produit vaut bien $(x^4 - 1)(x^4 + 1) = x^8 - 1$.
2. Pour calculer le dual du code $\mathcal{C}$, on commence par chercher à diviser $x^8 - 1$ par $g(x)$. Pour cela, on peut s'aider de la factorisation, ou simplement faire le calcul directement. On obtient

   $$x^8 - 1 = (x^2 - x - 1)g(x)\,,$$

   par conséquent $\mathcal{C}^\perp$ est engendré par le polynôme $g^\perp(x) = x^2 + x - 1$ (version unitaire du polynôme réciproque de $x^2 - x - 1$).
3. On remarque que $g^\perp(x)$ est un diviseur de $g(x)$, car $g(x) = (x-1)(x+1)(x^2+1)(x^2+x-1)$. Par conséquent, tout polynôme multiple de $g(x)$ est également un polynôme multiple de $g^\perp(x)$. En d'autres termes, tout mot de $\mathcal{C}$ est un mot de $\mathcal{C}^\perp$, ce qui signifie que $\mathcal{C} \subseteq \mathcal{C}^\perp$.
