Codes algébriques – Solutions feuille de TD 4

08/03/2024

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. ($\star$) 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.

Solutions de l'Exercice 1.

Solution Q1.

1. Les classes cyclotomiques sont : $C_1 = \{1, 2, 4, 8, 16\}$, $C_3 = \{3, 6, 12, 24, 17\}$ et $C_5 = \{5, 10, 20, 9, 18\}$, donc leur réunion est :
$$I = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 17, 18, 20, 24\}\,.$$
Cet ensemble admet une suite de 6 éléments consécutifs. La borne BCH assure donc que le code cyclique ainsi construit aura distance minimale $\geq 6 + 1 = 7$.
2. Les classes cyclotomiques sont : $C_0 = \{0\}$, $C_1 = \{1, 3\}$ et $C_5 = \{5, 7\}$, donc leur réunion est :
$$I = \{0, 1, 3, 5, 7\}\,.$$
Cet ensemble admet une suite de 3 éléments consécutifs modulo 8. En effet, $7 \equiv -1 \mod 8$, donc ces trois éléments sont -1, 0 et 1. La borne BCH assure donc que le code cyclique ainsi construit aura distance minimale $\geq 3 + 1 = 4$.

Solution Q2.

C'est un peu pénible, mais on va identifier les racines de $g(x)$ à la main. Puis, on appliquera ce que l'on a fait à la question précédente.

1. Observons que, comme $\deg(g) = 10$, on doit trouver 10 racines. Donnons d'abord la réprésentation polyomiale des puissances de α :

i	0	1	2	3	4	5	6	7	8
α^i	1	α	α^2	α^3	$\alpha+1$	$\alpha^2+\alpha$	$\alpha^3+\alpha^2$	$\alpha^3+\alpha+1$	α^2+1

i	9	10	11	12	13	14
α^i	$\alpha^3+\alpha$	$\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+\alpha$	$\alpha^3+\alpha^2+\alpha+1$	$\alpha^3+\alpha^2+1$	α^3+1

Puis, c'est parti pour les calculs...

— On a $g(1) = 1 \neq 0$, donc α^0 n'est pas racine.
— On a $g(\alpha) = (\alpha^2+\alpha+1)+(\alpha^2+1)+(\alpha^2+\alpha)+(\alpha+1)+\alpha^2+\alpha+1 = 0$, donc α^1 est une racine de g, donc tous ses conjugués le sont également, à savoir $\{\alpha^i \mid i \in C_1\}$ où $C_1 = \{1,2,4,8\}$.
— On a $g(\alpha^3) = 1+(\alpha^3+\alpha)+1+(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha^2)+\alpha^3+1 = 0$, donc α^3 est une racine de g, donc tous ses conjugués le sont également, à savoir $\{\alpha^i \mid i \in C_3\}$ où $C_3 = \{3,6,12,9\}$.
— En utilisant $\alpha^{15} = 1$, on a $g(\alpha^5) = \alpha^5+\alpha^{10}+\alpha^{10}+\alpha^5+\alpha^{10}+\alpha^5+1 = (\alpha^2+\alpha+1)+(\alpha^2+\alpha)+1 = 0$. Donc, α^5 est une racine de g, donc tous ses conjugués le sont également, à savoir $\{\alpha^i \mid i \in C_5\}$ où $C_3 = \{5,10\}$.
— On pourrait s'arrêter là, car on a trouvé 10 racines, mais on peut aussi vérifier que $g(\alpha^7) = 1$

L'ensemble de définition du code est donc :

$$I = \{1,2,3,4,5,6,8,9,10,12\}\,.$$

La borne BCH assure alors que le code a distance minimale ≥ 7.

2. Même méthode.

i	0	1	2	3	4	5	6	7	8	9	10	11
α^i	1	α	$2\alpha+1$	2	2α	$4\alpha+2$	4	4α	$3\alpha+4$	3	3α	$\alpha+3$

— On a $g(1) = 3 \neq 0$, donc α^0 n'est pas racine.
— Un calcul donne $g(\alpha^1) = 0$, donc $C_1 = \{1,5\}$ est dans l'ensemble de définition du code.
— Un calcul donne $g(\alpha^1) = 0$, donc $C_2 = \{2,10\}$ est dans l'ensemble de définition du code.
— On s'arrête là car on a trouvé 4 racines et le polynôme g est de degré 4.

L'ensemble de définition du code est donc $I = \{1,2,5,10\}$, donc la borne BCH assure que la distance minimale du code est ≥ 3.

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 ?

Solutions de l'Exercice 2.

Solution Q1.

1. Il faut d'abord choisir une racine primitive de l'unité. Dans l'exercice précédent, on a vu que $\alpha \in \mathbb{F}_{16}$ telle que $\alpha^4 = \alpha+1$ est satisfaisante. Pour obtenir la distante construite $\delta = 4$ avec un code BCH au sens strict, il faut réunir les classes cylcotomiques C_1, C_2 et C_3, puis faire le ppcm des polynômes minimaux associés. On remarque que $C_1 = C_2$, donc ont doit simplement calculer $M_1(x)M_3(x)$. Le polynôme $M_1(x)$ est le polynôme minimale de α, donc x^4+x+1. Le polynôme $M_3(x)$ vaut quant à lui :

$$\begin{aligned} M_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\ &= x^4 - (\alpha^3+\alpha^6+\alpha^{12}+\alpha^9)x^3 + (\alpha^9+\alpha^{15}+\alpha^{12}+\alpha^{18}+\alpha^{15}+\alpha^{21})x^2 - (\alpha^{27}+\alpha^{24}+\alpha^{21}+\alpha^{18})x + \alpha^{30} \\ &= x^4+x^3+x^2+x+1 \end{aligned}$$

Finalement, le polynôme générateur du code BCH voulu est

$$g(x) = M_1(x)M_3(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8+x^7+x^6+x^4+1\,.$$

2. On se place sur $\mathbb{F}_3$ avec $n = 13$. On choisit comme racine primitive de l'unité une racine de $P(x) = x^3+x^2+x+2$ (remarque : ce type de polynôme vous sera donné si besoin). Comme dans question précédente :
   — Comme la distance construite est $\delta = 5$ et le premier zéro est $b = 0$, l'ensemble de définition du code est la réunion des classes cyclotomiques de 0, 1, 2 et 3. On a $C_0 = \{0\}$ comme toujours, puis $C_1 = \{1,3,9\}$, $C_2 = \{2,6,5\}$ et $C_3 = C_1$.
   — Le polynôme générateur $g(x)$ du code BCH est alors le ppcm des polynômes minimaux associés à ces classes. Ces polynômes sont :

$$M_0(x) = x-\alpha^0 = x-1$$
$$M_1(x) = (x-\alpha)(x-\alpha^3)(x-\alpha^9) = x^3-(\alpha+\alpha^3+\alpha^9)x^2+(\alpha^4+\alpha^{10}+\alpha^{12})x-\alpha^{13} = x^3+x^2+x+2$$
$$M_2(x) = (x-\alpha^2)(x-\alpha^6)(x-\alpha^5) = x^3-(\alpha^2+\alpha^5+\alpha^6)x^2+(\alpha^7+\alpha^8+\alpha^{11})x-\alpha^{13} = x^3+x^2+2$$

   On obtient donc

$$g(x) = (x-1)(x^3+x^2+x+2)(x^3+x^2+2) = x^7+x^6-x^3+x^2-x+-1$$

Solution Q2.

1. L'ensemble de définition du premier code est $\{1,2,4,8,3,6,9,12\}$, donc la borne BCH donne en réalité $d \geq 5$.
2. L'ensemble dé définition du second code est $\{0,1,2,3,5,6,9\}$ donc la borne BCH donne toujours $d \geq 5$.

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.

Solutions de l'Exercice 3.

Solution Q1. Pour cela, deux méthodes. La première est de construire un polynôme générateur du code BCH, puis calculer le polynôme générateur du dual et enfin construire la matrice. Nous avons déjà fait ce type de calcul dans un TD précédent.

La **seconde méthode**, vue en cours, consiste à créer une matrice de partité du code sur une extension de corps $\mathbb{F}_q^m$, de décomposer chaque coefficient de la matrice sur $\mathbb{F}_q$, puis de réduire la matrice obtenue. Optons pour cette méthode.

Choisissons $\alpha \in \mathbb{F}_9$ tel que $\alpha^2+\alpha-1 = 0$. On a la table suivante :

i	0	1	2	3	4	5	6	7
α^i	1	α	$-\alpha+1$	$-\alpha-1$	-1	$-\alpha$	$\alpha-1$	$\alpha+1$

Par construction, la matrice

$$\boldsymbol{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} \end{pmatrix}$$

est une matrice de parité du code. Décomposons chaque élément de $\mathbb{F}_9$ sur $\mathbb{F}_3$:

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

La matrice obtenue est de rang 4 (calcul un peu pénible) : par exemple on peut observer que la 6-ème ligne est égale à la l'opposée de la 2-ème, et que la somme de la 1-ère et de la 6-ème ligne donne la 5-ème ligne.

Une matrice de parité du code BCH est donc :

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

Solution Q2. Même idée (à faire)

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

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

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

Question 2.– Démontrer que $I' = \left\{ (-i) \mod n \mid i \in \{0, \dots, n-1\} \setminus I \right\}$ 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.

Solutions de l'Exercice 4.

Solution Q1.
