T. D. Codes correcteurs d'erreurs.
POLYTECH. 4ième année
AIX-MARSEILLE UNIVERSITÉ
Année universitaire 2019/2021

Enseignants : Alexis Bonnecaze
Odile Papini

Feuille de T. D. 3 corrigée : Codes cycliques

Exercice 1 : code cyclique

I)
Soit C un code cyclique de longueur 15 sur $\mathbb{F}_2$ de polynôme générateur $g(x) = x^4 + x + 1$.

1) La dimension du code est $n - deg(g(x)) = 15 - 4 = 11$.

2) Le polynôme générateur de l'orthogonal du code C est $x^k h(^{-1})$ où $h(x)$ est le polynôme de contrôle, c'est à dire qu'il est tel que $x^{15} - 1 = g(x).h(x)$.

   La division de $x^{15} - 1$ par $g(x)$ donne
   $h(x) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$ et
   $x^{11} h(^{-1}) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$.

3) La matrice de contrôle du code C est

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

4) La distance minimale du code C est $d = 3$. Il n'existe pas de mot de poids 1 car il n'y a pas de colonne nulle dans H. Il n'y a pas de mot de poids 2 car il n'y a pas deux colonnes égales dans H. En revanche, il y a des mots de poids 3 il existe des colonnes de H combinaisons linéaires de 2 colonnes de H. Par exemple, $c_5 = c_1 + c_2$.

Exercice 2 : code de Hamming

Nous avons montré (voir feuille de TD 2) que le code de Hamming sur $\mathbb{F}_2$ est un code de longueur $2^m - 1$, de dimension $2^m - 1 - m$ et de distance minimale $d = 3$, admettant pour matrice de contrôle une matrice dont les $2^m - 1$

colonnes sont tous les m-uplets non nuls de $\mathbb{F}_2$. Soit α un élément primitif de $\mathbb{F}_{2^m}$ alors les éléments du corps $\mathbb{F}_{2^m}$, c'est à dire $1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}$ peuvent être représentés par les m-uplets non nuls de $\mathbb{F}_2$.

1) Montrer qu'un code de Hamming est un code cyclique de polynôme gérateur $g(x) = M^{(1)}(x)$ où $M^{(1)}(x)$ est le polynôme minimal de α.

   Soit $\mathbb{F}_2^m = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$, les éléments non nuls de $\mathbb{F}_2^m$ peuvent être représentés par des m-uplets distincts non nuls et la matrice H du code de Hamming peut s'écrire :

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \end{pmatrix}$$

   où chaque m-uplet est remplacé par un élément de $\mathbb{F}_{2^m}$.

   Soit $c = (c_0, \cdots c_{n-1})$ appartient au code de Hamming si et seulement si $Hc^t = 0$ si et seulement si $\Sigma_{i=0}^{n-1} c_i \alpha^i = 0$ si et seulement si $c(\alpha) = 0$.

   Par définition un polynôme minimal de α sur $\mathbb{F}_2$ est tel que c'est un polynôme de plus petit degré à coefficients dans $\mathbb{F}_2$ tel que $M(\alpha) = 0$.

   Soit $c(\alpha) = 0$ on a $M(x)$ divise $c(x)$. En effet, $c(x) = M(x).a(x) + r(x)$ avec $deg(r(x)) < deg(M(x))$.

   $c(\alpha) = M(\alpha).a(\alpha) + r(\alpha)$

   $0 = 0 + r(\alpha)$

   si $r(\alpha) = 0$, $r(x)$ est un polynôme de degré inférieur au degré de $M(x)$ ayant α pour racine. Ce qui contredit la définition du polynôme minimal donc $r(x) = 0$ et donc $M(x)$ divise $c(x)$.

2) Donner une matrice génératrice du code de Hamming sur $\mathbb{F}_2$ est un code de longueur $2^m - 1$.

$$G = \begin{pmatrix} M(x) & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & xM(x) & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & x^2M(x) & \cdots & 0 \\ 0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & x^{n-m-1}M(x) \end{pmatrix}$$

3) Lorsque $m = 3$ vérifier que les lignes de H sont orthogonales aux lignes de G.

$\mathbb{F}_2^3 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ et $M(x) = x^3 + x + 1$.

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

Exercice 3 : corps fini

On souhaite décomposer $x^8 - 1$ sur $\mathbb{F}_3$.

1) On considère le corps $\mathbb{F}_3$, le corps à trois éléments. Construire les tables d'addition et de multiplication de ce corps.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2) Le sur-corps de décomposition de $x^8 - 1$ sur $\mathbb{F}_3$ est tel que m est le plus petit entier tel que n divise $3^m - 1$. Donc $m = 2$ et le corps de décomposition est $F_{3^2} = F_9$.
$F_9 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$.
Le corps F_9 est engendré par le polynôme primitif $x^2 + x + 2$ et
$\alpha^2 = 2\alpha + 1$
$\alpha^3 = 2\alpha + 2$
$\alpha^4 = 2$
$\alpha^5 = 2\alpha$
$\alpha^6 = \alpha + 2$
$\alpha^7 = \alpha + 1$.

3) Décomposer $x^8 - 1$ sur $\mathbb{F}_3$.

On cherche les classes cyclotomiques $i, i.3, i.3^2, \cdots (mod 8)$

$classe\ de\ 0: \rightarrow 0 \quad (x-\beta^0)$
$classe\ de\ 1: \rightarrow 1,3 \quad (x-\beta^1)(x-\beta^3)$
$classe\ de\ 2: \rightarrow 2,6 \quad (x-\beta^2)(x-\beta^6)$
$classe\ de\ 4: \rightarrow 4 \quad (x-\beta^4)$
$classe\ de\ 5: \rightarrow 5,7 \quad (x-\beta^5)(x-\beta^7)$

On cherche ensuite à quel élément de F_9 correspond β, il est tel que $\beta^{3^m-1} = \alpha^{ns}$, ns divise $3^m - 1$, ici $n = 1$ et $\beta = \alpha$.

$(x-\beta^0) = (x-1)$

$(x-\beta^1)(x-\beta^3) = (x-\alpha^1)(x-\alpha^3)$ en faisant les calculs dans F_9, on trouve $x^2 - 2x + 2$.

$(x-\beta^2)(x-\beta^6) = (x-\alpha^2)(x-\alpha^6)$ en faisant les calculs dans F_9, on trouve $x^2 + 1$.

$(x-\beta^4) = (x-\alpha^4)$ en faisant les calculs dans F_9, on trouve $x - 2$.
$(x-\beta^5)(x-\beta^7) = (x-\alpha^5)(x-\alpha^7)$ en faisant les calculs dans F_9, on trouve $x^2 - x + 2$.

Donc $x^8 - 1 = (x-1)(x^2-2x+2)(x^2+1)(x-2)(x^2-x+2)$.

4) Quels sont les codes cycliques de longueur 8 sur $\mathbb{F}_3$?

Les polynômes générateurs des codes cycliques de longueur 8 sur $\mathbb{F}_3$ sont classés par degré dans les tables ci-dessous.

1	2	3	4
$(x-1)$	(x^2-2x+2)	$(x-1)(x^2-2x+2)$	$(x-2)(x-1)(x^2-2x+2)$
$(x-2)$	(x^2-x+2)	$(x-1)(x^2-x+2)$	$(x-2)(x-1)(x^2-x+2)$
	(x^2+1)	$(x-1)(x^2+1)$	$(x-2)(x-1)(x^2+1)$
	$(x-1)(x-2)$	$(x-2)(x^2-2x+2)$	$(x^2-2x+2)(x^2-x+2)$
		$(x-2)(x^2-x+2)$	$(x^2-2x+2)(x^2+1)$
		$(x-1)(x^2+1)$	$(x^2-x+2)(x^2+1)$

5	6
$(x-1)(x^2-2x+2)(x^2-x+2)$	$(x^2-2x+2)(x^2-x+2)(x^2+1)$
$(x-1)(x^2-2x+2)(x^2+1)$	$(x^2-2x+2)(x^2-x+2)(x-1)(x-2)$
$(x-1)(x^2-2x+2)(x^2+1)$	$(x^2-2x+2)(x^2+1)(x-1)(x-2)$
$(x-2)(x^2-2x+2)(x^2-x+2)$	$(x^2-x+2)(x^2+1)(x-1)(x-2)$
$(x-2)(x^2-2x+2)(x^2+1)$	
$(x-2)(x^2-2x+2)(x^2+1)$	

7
$(x^2-2x+2)(x^2-x+2)(x^2+1)(x-1)$
$(x^2-2x+2)(x^2-x+2)(x^2+1)(x-2)$

Exercice 4 **: code BCH**

Soit le polynôme sur $\mathbb{F}_2$, $g(x) = x^8 + x^7 + x^6 + x^4 + 1$.

1) $g(x)$ est un polynôme générateur d'un code cyclique C de longueur 15 car $g(x)$ divise $x^{15}-1$, $x^{15}-1 = (x^8+x^7+x^6+x^4+1)(x^7+x^6+x^4+1)$.

2) Quelle est la dimension de C ?

   $dim(C) = n - deg(g(x)) = 7$

3) Montrer que C est un code BCH.

   $g(x) = x^8 + x^7 + x^6 + x^4 + 1 = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)$, or $x^4 + x + 1$ est le polynôme minimal de α, noté $M^{(1)}_{(x)}$, $\alpha \in F_{16}$, et $x^4+x^3+x^2+x+1$ est le polynôme minimal de α^3, noté $M^{(3)}_{(x)}$, $\alpha^3 \in F_{16}$.

   $M^{(1)}_{(x)}$ a pour racines : α, α^2, α^4, α^8.

   $M^{(3)}_{(x)}$ a pour racines : α^3, α^6, α^9, α^{12}.

   Il y a 4 racines dont les exposants sont des entiers consécutifs, donc $\delta - 1 = 4$, c'est un code BCH de distance construite $\delta = 5$.

4) Quelle la distance construite de C ?

   $\delta = 5$.

5) Quelle la distance minimale de C ? Quelle est sa capacité de correction ?

$\delta = d = 5$ car $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ permet de construire un mot de poids 5.

La capacité de correction de C est $e = \lfloor (d-1)/2 \rfloor$.

Exercice 5 : code Reed-Solomon

Le but de cet exercice est de construire un code de Reed-Solomon de longueur 7 et de distance minimale 5, noté C.

1) Les paramètres d'un code de Reed-Solomon sont $n = 2^m - 1$, $k = 2^m - 1 - r$, $d = r + 1$.

$n = 7$ donc $m = 3$ et C est un code de Reed-Solomon sur $\mathbb{F}_8$ engendré par le polynôme primitif $f(x) = x^3 + x + 1$.

$x^7 - 1 = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$ sur $\mathbb{F}_8$.

On souhaite un code de Reed-Solomon avec $d = 5$ donc $r = 4$ et $k = 7 - 4 = 3$ donc $deg(g(x) = n - k = 4$ donc lepolynôme générateur du code C est$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$ et $g(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$.

2) La matrice génératrice du code C.

$$G = \begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix}$$

3) Les paramètres du code, noté IC, qui est l'image binaire du code C. Pour l'image binaire : 0 est remplacé par 000, 1 est remplacé par 100, α est remplacé par 010, $\cdots$.

La longueur de IC est $n = 21$, la dimension de IC est $k = 9$.

4) Le nombre de mots du code IC est 2^9.

PS: A toutes fins utiles on rappelle que le corps $\mathbb{F}_9$ est engendré par le polynôme primitif $f(x) = x^2 + x + 2$ et que le corps $\mathbb{F}_{16}$ est engendré par le polynôme primitif $f(x) = x^4 + x + 1$.