T. D. Codes correcteurs d'erreurs.
POLYTECH. 4ième année
UNIVERSITÉ D'AIX-MARSEILLE
Année universitaire 2017/2018

Enseignants : Alexis Bonnecaze
Odile Papini

Feuille de T. D. 3 corrigée : Codes cycliques

Exercice 1 : code cyclique

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 $x^k h(-x)$ 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
   $x^{11}h(-x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$.

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, $c_5 = c_1 + c_4$.

Exercice 2 : Code Simplexe

Nous avons vu (voir feuille de TD 2) qu'un code Simplexe sur $\mathbb{F}_2$ est un code de longueur $2^m - 1$, de dimension m et de distance minimale 2^{m-1}, admettant pour matrice génératrice une matrice G $(m \times 2^m - 1)$ dont les

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 $\mathbb{F}_2$.

I) Montrer qu'un code Simplexe est un code cyclique. Nous avons vu dans le TD 2 que le code Simplexe est un code linéaire qui est le dual (orthogonal) d'un code de Hamming, comme nous avons vu en cours que le de Hamming est un code cyclique, et qu'il est montré que le dual (orthogonal) d'un code cyclique est cyclique, le code Simplexe est un code cyclique.

II) Donner le polynôme générateur du code Simplexe.

   Nous savons que le code de Hamming est un code $(2^m-1, 2^m-1-m, 3)$, nous avons vu en cours que son polynôme générateur est $g_H(x) = M^{(1)}(x)$. Son polynôme de contrôle $h_H(x)$ est tel que $g_H(x).h_H(x) = x^{2^m-1} - 1$, donc $h_H(x)$ est le reste de la division de $x^{2^m-1} - 1$ (modulo $x^{2^m-1}-1$) par $g_H(x)$. Comme le code Simplexe est l'orthogonal du code de Hamming, le polynôme générateur du code Simplexe est $g_S(X) = x^{2^m-1-m} h_H(x^{-1})$

III) Lorsque $m = 3$

   1) Donner les polynômes générateur et de contrôle du code Simplexe. Lorsque $m = 3$, le code Simplexe a pour paramètres (7,3,4) et le code de Hamming a pour paramètres (7,4,3), le polynôme générateur du code de Hamming est $g_H(x) = x^3 + x + 1$ et $x^7 - 1 = (x^3 + x + 1).(x^4 + x^2 + x + 1)$ donc le polynôme de contrôle du code de Hamming est $h_H(x) = x^4 + x^2 + x + 1$, en conséquence $g_S(X) = x^4 h_H(x^{-1}) = x^4 + x^3 + x^2 + 1$

   2) Donner une matrice une matrice génératrice G_S et une matrice de contrôle H_S du code Simplexe.

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

   Elle correspond à

$$G_S = \begin{pmatrix} 1 & \alpha & \alpha^6 & \alpha^3 & \alpha^5 & \alpha^4 & \alpha^2 \end{pmatrix}$$

et

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

3) Vérifier que les lignes de H_S sont orthogonales aux lignes de G_S.

Exercice 4 : codes cycliques

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

   Le polynôme de contrôle de C est $h(x) = x^7 + x^6 + x^4 + 1$, la matrice de contrôle est donc :

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

   Il n'existe pas de mot de poids 1, 2, 3, 4 mais il existe un mot de poids 5 car $c_2 + c_3 + c_4 + c_{11} + c_{15} = 0$. Donc $d = 5$ et $e = \lfloor (d-1)/2 \rfloor = 2$.