Introduction à la théorie des codes correcteurs d'erreurs

Codes cycliques

Odile PAPINI

POLYTECH
Université d'Aix-Marseille
odile.papini@univ-amu.fr
http://odile.papini.perso.luminy.univ-amu.fr/sources/CODAGE.html

Plan du cours

Bibliographie I


J. Mac Willians & N. J. A. Sloane
Error Correcting codes.
, ed. 19.


O. Papini & J. Wolfmann
Algèbre discrète et codes correcteurs d'erreurs.
Springer Verlag, ed. 1995.


Support de cours
Claude Carlet Université Paris 13
http://www.math.univ-paris13.fr/ schartz/Mali/Mali07/ccc.pdf

définition et représentation des codes cycliques

définition : code cyclique

Soit C un code sur un corps fini $\mathbb{K}$ un code C est dit **cyclique** si :

- i) C est un code linéaire;
- ii) Si $(x_1, \cdots, x_n) \in C$, alors $(x_n, x_1, \cdots x_{n-1}) \in C$.

Exemple : Soit C le code de matrice génératrice

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

La permutation circulaire des composantes vers la droite transforme chaque mot du code en un mot du code

représentation polynômiale

Soit C un code linéaire de longueur n
A chaque mot m de C on associe un polynôme $m(x)$

$$m = (a_0, a_1, \cdots, a_{n-1}) \quad \rightarrow \quad m(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$$

$$(a_{n-1}, a_0, \cdots, a_{n-2}) \quad \rightarrow \quad a_{n-1} + a_0 x + \ldots + a_{n-2} x^{n-1}$$

or

$$a_{n-1} + a_0 x + \ldots + a_{n-2} x^{n-1} = x.m(x) \text{ modulo } \mathrm{x^n} - 1$$

caractérisation

C est cyclique ssi $\forall m \in C, \quad x.m(x)$ **modulo** $x^n - 1$
est la représentation polynômiale de C

représentation polynômiale

définition

La représentation polynômiale d'un code C, notée $C(x)$, est l'ensemble des représentations polynômiales $m(x)$ des mots m de C

propriétés

- **si** $x.m(x) \in C(x)$ **alors** $\forall i \in \mathbb{N},\ x^i.m(x) \in C(x)$
- C **est cyclique ssi tout multiple modulo** $x^n - 1$ **d'un polynôme de** $C(x)$ **est aussi dans** $C(x)$

rappels d'algèbre

Rappel : notion d'idéal

Si A est un anneau commutatif,

un idéal de A est une partie I de A telle que :

- I est un sous-groupe additif de A
- $\forall a \in A$ et $\forall i \in I$, le produit $a.i \in I$

définition code cyclique

Soit C un code linéaire sur K

- $\mathbb{K}[x]/(x^n - 1)$ est un anneau commutatif
- l'application Θ:
  $(a_0, a_1, \cdots, a_{n-1}) \rightarrow m(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ est un isomorphisme d'Espace Vectoriel
- $C(x) = \Theta(C)$ est un **sous groupe additif** de $\mathbb{K}[x]/(x^n - 1)$
- C **est cyclique ssi** $C(x)$ **est un idéal**

définition code cyclique

théorème

C est cyclique ssi $C(x)$ est un idéal de $\mathbb{K}[x]/(x^n - 1)$

consèquence

rechercher tous les codes cycliques de longueur n sur K revient à rechercher tous les idéaux de $\mathbb{K}[x]/(x^n - 1)$

Rappels d'algèbre : notion d'idéal principal

rappel : d'idéal principal

Soit $\mathbb{K}$ un corps et n un entier non nul de $\mathbb{N}$

- un idéal est principal s'il est formé de tous les multiples d'un même élément
- tout idéal de $\mathbb{K}[x]$ est un idéal principal
- tout idéal de $\mathbb{K}[x]/(x^n - 1)$ est un idéal principal

théorème

La représentation polynômiale dans $\mathbb{K}[x]/(x^n - 1)$ d'un code cyclique est formée par **tous les multiples d'un même polynôme**. On l'appelle le **générateur** du code cyclique

théorème

Chaque code cyclique de longueur n sur $\mathbb{K}$, non réduit à $\{0\}$, possède **un générateur et un seul qui est un diviseur de** $x^n - 1$ **dans** $\mathbb{K}[x]$, et dont le coefficient dominant est 1 (i.e. le polynôme est **unitaire**).

dimension et matrice génératrice d'un code cyclique

Soit C un code cyclique de longueur n sur K, et soit $g(x)$ le générateur de degré t de C. Tout polynôme de $C(x)$ est de la forme $a(x).g(x)$:

$$(a_0 + a_1x + \ldots + a_sx^s)g(x) = a_0g(x) + a_1xg(x) + \ldots + a_sx^sg(x)$$
$$0 \leq s \leq n-1$$

Les polynômes $g(x), xg(x), \ldots, x^{n-1}g(x)$ forment donc une famille génératrice de $C(x)$ dont on extrait une base :

théorème

La dimension d'un code cyclique de longueur n,dont le générateur est $g(x)$, est $k = n - \deg g(x)$

matrice génératrice d'un code cyclique

théorème

Soit $g(x) = g_0 + g_1 x^1 + \ldots + g_t x^t$ le générateur d'un code cyclique C de longueur n sur $\mathbb{K}$. La matrice G à k lignes et n colonnes suivante, où $t = \deg g(x) = n - k$, est une matrice génératrice de C :

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_t & 0 & \cdots & \cdots & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_t & 0 & \cdots & 0 & 0 \\ \vdots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_t & 0 \\ 0 & 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_t \end{pmatrix}$$

Le codage consiste à multiplier $g(x)$ par des polynômes de degré au plus $k - 1$

orthogonal d'un code cyclique

Soit $g(x)$ le générateur de C, et $t = \deg g(x)$.
L 'orthogonal de C a pour dimension $n - dim(C) = n - (n - t) = t$.

définition

On appelle **polynôme de contrôle**, le polynôme $h(x)$ tel que $x^n - 1 = g(x)h(x)$

théorème

Soit C un code cyclique. Alors :

- i) L'orthogonal d'un code cyclique C est un code cyclique;
- ii) Si $h(x)$ est le polynôme de contrôle de C, alors le générateur de l'orthogonal de C est $x^k h(x^{-1})$;

orthogonal d'un code cyclique

théorème (suite)

Soit C un code cyclique. Alors :

- iii) Si $h(x) = \Sigma_{j=0}^{k} h_j x^j$ alors la matrice de contrôle de C est :

$$\begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & \cdots & \cdots & 0 \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{pmatrix}$$

remarque : L'orthogonal de C est équivalent au code engendré par le polynôme de contrôle

Rappels sur les corps finis

$\{0, 1, \cdots n-1\}$ muni de la somme modulo n et du produit modulo n est un anneau commutatif unitaire : $\mathbb{Z}/n\mathbb{Z}$

corps finis

$\mathbb{Z}/n\mathbb{Z}$ est un corps ssi n est premier

Existe-il d'autres corps finis ?

corps finis

Réponse d'Evariste Galois : OUI
(de cardinalité puissance d'un nombre premier)

Comment les construire ?

Construction des corps finis

$\mathbb{K}[x]$: ensemble de polynômes sur $\mathbb{K}$ corps fini et $f(x) \in \mathbb{K}[x]$
$\mathbb{K}[x]$ muni de la somme des polynômes modulo $f(x)$ et du produit des polynômes modulo $f(x)$ est un anneau commutatif unitaire :

$$\mathbb{K}[x]/f(x)$$

corps finis

$\mathbb{K}[x]/f(x)$ est un corps ssi $f(x)$ est irréductible sur $\mathbb{K}$

$f(x)$ est un polynôme irréductible sur $\mathbb{K}$ si

- $deg(f(x)) > 0$
- $f(x)$ est divisible par λ et $\lambda.f(x)$ avec $\lambda \in \mathbb{K}^*$

exemple 1 : construction d'un corps à 4 éléments

$\mathbb{K} = \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2 = \{0, 1\}$ et $f(x) = x^2 + x + 1$

$\mathbb{K}[x]/f(x) = \{0, 1, x, 1 + x\}$ est un corps noté $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$

$$\begin{array}{rl} 0 & \Rightarrow 0 \\ 1 & \Rightarrow 1 \\ x & \Rightarrow \alpha \\ 1 + x & \Rightarrow \alpha^2 \end{array}$$

- α est un élément primitif de $\mathbb{F}_4$
- $f(\alpha) = 0 \Rightarrow \alpha^2 = 1 + \alpha$
- $\mathbb{F}_2 \subset \mathbb{F}_4$

exemple 1 : propriétés des corps finis

$\mathbb{F}_2 = \{0, 1\}$ et $f(x) = x^2 + x + 1$ irréductible sur $\mathbb{F}_2$

$\mathbb{F}_4 = \mathbb{F}_2[x]/f(x)$

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$

- α est un élément primitif de $\mathbb{F}_4$
- tous les éléments non nuls sont puissance de α
- α est racine de $f(x)$ sur $\mathbb{F}_4$
- $f(\alpha) = 0 \Rightarrow \alpha^2 = 1 + \alpha$
- $(1, \alpha)$ base de $\mathbb{F}_4$ espace vectoriel sur $\mathbb{F}_2$

exemple 2 : construction d'un corps à 8 éléments

$\mathbb{K} = \mathbb{F}_2 = \{0, 1\}$ et $f(x) = x^3 + x + 1$

$\mathbb{K}[x]/f(x) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ est un corps
noté $\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

$$\begin{array}{cc} 0 & \Rightarrow 0 \\ 1 & \Rightarrow 1 \\ x & \Rightarrow \alpha \\ x^2 & \Rightarrow \alpha^2 \\ x+1 & \Rightarrow \alpha^3 \\ x^2+x & \Rightarrow \alpha^4 \\ x^2+x+1 & \Rightarrow \alpha^5 \\ x^2+1 & \Rightarrow \alpha^6 \end{array}$$

- α est un élément primitif de $\mathbb{F}_8$
- $f(\alpha) = 0 \Rightarrow \alpha^3 = 1 + \alpha$
- $\mathbb{F}_2 \subset \mathbb{F}_8$

exemple 2 : propriétés des corps finis

$\mathbb{F}_2 = \{0, 1\}$ et $f(x) = x^3 + x + 1$ irréductible sur $\mathbb{F}_2$

$\mathbb{F}_8 = \mathbb{F}_2[x]/f(x)$

$\mathbb{F}_8 = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$

- α est un élément primitif de $\mathbb{F}_8$
- tous les éléments non nuls sont puissance de α
- α est racine de $f(x)$ sur $\mathbb{F}_8$
- $f(\alpha) = 0 \Rightarrow \alpha^3 = 1 + \alpha$
- $(1, \alpha, \alpha^2)$ base de $\mathbb{F}_8$ espace vectoriel sur $\mathbb{F}_2$

Un exemple : le code de Hamming

Code de Hamming sur $\mathbb{F}_2$

- longueur : $n = 2^m - 1$,
- dimension : $k = 2^m - 1 - m$
- distance minimale : $d = 3$
- matrice de contrôle : les $2^m - 1$ colonnes sont tous les m-uplets non nuls de $\mathbb{F}_2$.

Le code de Hamming est cyclique

corps fini $\mathbb{F}_{2^m}$

α : élément primitif de $\mathbb{F}_{2^m}$
$\mathbb{F}_{2^m} = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$
les éléments non nuls de $\mathbb{F}_2^m$: $1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}$ peuvent être représentés par les m-uplets non nuls de $\mathbb{F}_2$.

matrice H du code de Hamming

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

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

$c = (c_0, \cdots c_{n-1})$ appartient au code de Hamming ssi $Hc^t = 0$

$$\text{ssi} \qquad \sum_{i=0}^{n-1} c_i \alpha^i = 0 \qquad \text{ssi} \qquad c(\alpha) = 0$$

Le code de Hamming est cyclique

polynôme minimal de α sur $\mathbb{F}_2$

polynôme de plus petit degré à coefficients dans $\mathbb{F}_2$ tel que $M(\alpha) = 0$.

Soit $c(x)$ tel que $c(\alpha) = 0$

$$M(x) \text{ divise } c(x).$$

$c(x) = M(x).a(x) + r(x)$ avec $deg(r(x)) < deg(M(x))$.
or
$c(\alpha) = M(\alpha).a(\alpha) + r(\alpha)$ et $r(\alpha) = 0$
si $r(\alpha) = 0$ alors $r(x)$ 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 $c(x)$.

Le code de Hamming est cyclique

Pour toute representation polynomiale $c(x)$ d'un mot du code de Hamming $M(x)$ divise $c(x)$.

polynôme générateur du code de Hamming

$$M(x)$$

matrice de génératrice du code de Hamming

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

Le code de Hamming est cyclique

cas m=3

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

$\mathbb{F}_{2^3} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ 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

Vérifier que les lignes de H sont orthogonales aux lignes de G.