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.esil.univmed.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

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

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

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

Propriétés des corps finis

Soit $\mathbb{F}_q$ un corps fini tel que $q = p^r$ avec p premier,

propriété

- si $q = p^r$, $\mathbb{F}_q$ contient un sous-corps isomorphe à $\mathbb{F}_p$ (corps de base)
- $\forall x \in \mathbb{F}_q \quad p.x = 0$ (p caractéritique du corps)
- $\forall x \in \mathbb{F}_q \quad x^q = x$
- $\forall s \in \mathbb{N}, \forall x, y \in \mathbb{F}_q \quad (x+y)^{p^s} = x^{p^s} + y^{p^s}$

Propriétés des corps finis

propriétés (suite)

- si $\mathbb{F}_q = \mathbb{K}[x]/f(x)$ avec $\mathbb{K} = \mathbb{F}_p$, p premier et $f(x)$ irréductible sur $\mathbb{K}$ alors $f(x)$ possède au moins une racine dans $\mathbb{F}_q$
- le groupe multiplicatif de de $\mathbb{F}_q$ est cyclique (tous les éléments sont puissance d'un même élément (**élément primitif**))
- si α est un élément primitif de $\mathbb{F}_q$, $q = p^r$ alors tout élément de $\mathbb{F}_q$ est une C. L. d'une manière unique de $1, \alpha, \alpha^2, \cdots, \alpha^{r-1}$
- $(1, \alpha, \cdots, \alpha^{r-1})$ est une base de $\mathbb{F}_q$ espace vectoriel sur $\mathbb{F}_p$

exemple : propriété des corps fini

$\mathbb{F}_2 = \{0, 1\}$ 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 $\mathbb{F}_2$

décomposition de $x^n - 1$ sur $\mathbb{F}_q$: n premier avec p (1)

Soit $n \in \mathbb{N}^*$, q une puissance d'un nombre premier p, $\mathbb{K} = \mathbb{F}_q$ le corps fini

- Il existe un corps fini $\mathbb{L}$ qui contient $\mathbb{K}$ et sur lequel $x^n - 1$ se décompose en n facteurs de degré 1. (Corps de décomposition de $x^n - 1$ sur $\mathbb{K}$);
- Dans $\mathbb{L}$, le polynôme $x^n - 1$ a donc n racines distinctes, ce sont les **racines $n$ièmes de l'unité dans $\mathbb{K}$**;
- Si m est le plus petit entier tel que n divise $q^m - 1$, alors $\mathbb{L} = \mathbb{F}_{q^m}$. Le corps $\mathbb{L}$ s'appelle le **corps des racines $n$ièmes de l'unité sur $\mathbb{F}_q$**;

décomposition de $x^n - 1$ sur $\mathbb{F}_q$: n premier avec p (2)

Soit $n \in \mathbb{N}^*$, q une puissance d'un nombre premier p, $\mathbb{K} = \mathbb{F}_q$
$\mathbb{L}$ le **corps des racines *n*ièmes de l'unité sur** $\mathbb{F}_q$

- Les racines de $x^n - 1$ forment un sous-groupe cyclique d'ordre n du groupe multiplicatif de $\mathbb{L}$, c'est à dire qu'elles sont toutes des puissances de l'une d'entre elles qui est, par définition, une *racine nième primitive* de l'unité;

- Si $ns = q^m - 1$ et α est une racine primitive de $\mathbb{L}$, on peut choisir comme racine *n*ième primitive de l'unité : $\beta = \alpha^s$

décomposition de $x^n - 1$ sur $\mathbb{F}_q$: n premier avec p (3)

si $x^n - 1 = f_0(x)f_1(x)\cdots f_{t-1}(x)$

- Chaque racine $n$ième de l'unité u est une racine d'un polynôme $f_i(x)$ et un seul.

  C'est le polynôme unitaire de plus petit degré sur $\mathbb{K}$, irréductible sur $\mathbb{K}$, qui admet u comme racine dans $\mathbb{L}$. C'est donc **le polynôme minimal** de u

- Si $f_i(x)$ est le polynôme minimal de u, les racines de $f_i(x)$ sont les conjugués de u : Soit $u, u^q, u^{q^2}, \ldots, u^{q^{s-1}}$ (où s est le degré de $f_i(x)$)

Le cycle $(i, iq, iq^2, \ldots, iq^j, \ldots)$ s'appelle la **classe cyclotomique de** i (relative à q modulo n)

algorithme de décomposition

algorithme

- 1) Détermination du plus petit entier m tel que n divise $q^m - 1$. On en déduit le corps des racines $n$ièmes de l'unité sur $\mathbb{F}_q$, soit $\mathbb{L} = \mathbb{F}_{q^m}$;

- 2) Détermination des différentes classes cyclotomiques $(i, iq, iq^2, \ldots, iq^j, \ldots)$. Leur nombre est celui des facteurs irréductibles cherchés, et le nombre d'éléments dans une classe est le degré du polynôme correspondant;

- 3) Pour chaque classe cyclotomique, détermination du polynôme correspondant. (En utilisant les opérations dans le corps $\mathbb{L}$ ou toute autre méthode)

exemple : décomposition de $x^5 - 1$ sur $\mathbb{F}_2$ (1)

$n = 5$ recherche de m le plus petit entier divisant $2^m - 1$ $m = 4$,
$\mathbb{L} = \mathbb{F}_{2^4} = \mathbb{F}_{16}$

$\mathbb{F}_{16} = \mathbb{F}_2[x]/f(x)$ avec $f(x) = x^4 + x + 1$

$\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \cdots, \alpha^{14}\}$
$(1, \alpha, \alpha^2, \alpha^3)$ est une base de $\mathbb{F}_{16}$ sur $\mathbb{F}_2$

α élément primitif racine de $f(x)$ sur $\mathbb{F}_{16}$, $f(\alpha) = 0 \Rightarrow \alpha^4 = 1 + \alpha$,
$\alpha^5 = \alpha + \alpha^2$, $\alpha^6 = \alpha^2 + \alpha^3$, $\alpha^7 = 1 + \alpha + \alpha^3$, etc $\cdots$

Exercice : construire une table d'addition et de multiplication pour $\mathbb{F}_{16}$

exemple : décomposition de $x^5 - 1$ sur $\mathbb{F}_2$ (2)

$\mathbb{L} = \mathbb{F}_{16}$, α racine primitive de $\mathbb{F}_{16}$, β racine primitive de l'unité
$\beta = \alpha^s$ avec $5.s = 2^m - 1$, $s = 3$ et $\beta = \alpha^3$
Les racines 5ièmes primitives de l'unité sont :
$\beta^0 = 1$, $\beta^1 = \alpha^3$, $\beta^2 = \alpha^6$, $\beta^3 = \alpha^9$, $\beta^4 = \alpha^{12}$

$x^5 - 1 = (x - \beta^0)(x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)$
classes cyclotomiques :
$(0) : 0 \Rightarrow f_0(x) = x - 1$
$(1) : 1, 2, 3, 4 \Rightarrow f_1(x) = (x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)$

$f_1(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^9)(x - \alpha^12)$
calculs dans $\mathbb{F}_{16}$: $f_1(x) = x^4 + x^3 + x^2 + x + 1$

$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$

décomposition de $x^n - 1$ sur $\mathbb{F}_q$: n non premier avec p

$n = mp^v$ $\quad$ m est premier avec p, $\quad$ $v \geq 1$

$$x^n - 1 = x^{mp^v} - 1 = (x^m - 1)^{p^v}$$

décomposer $x^m - 1$ avec la méthode du premier cas

codes BCH (Bose Chaudhuri Hocquemghen)

théorème des codes BCH

Soit C un code cyclique de longueur n sur $\mathbb{F}_q$ de polynôme générateur $g(x)$, avec n premier q.

Soit δ un entier $\delta \geq 1$ et β une racine primitive nième de l'unité sur $\mathbb{L}$ le corps de décomposition de $x^n - 1$ sur $\mathbb{F}_q$

Si $g(x)$ possède parmi ses racines dans $\mathbb{L}$ $(\delta - 1)$ puissances de β dont les exposants sont des entiers consécutifs,
$\beta^r, \beta^{r+1}, \cdots, \beta^{r+\delta-2}$ alors le poids minimum du code C est au moins δ

codes BCH exemple

Décomposition de $x^9 - 1$ sur $\mathbb{F}_2$ (laissée en exercice)
$x^9 - 1 = (x-1)(x^6 + x^3 + 1)(x^2 + x + 1)$
$\mathbb{L} = \mathbb{F}_{64}$ avec $f(x) = x^6 + x + 1$
les classes cyclotomiques sont (0), (1, 2, 4, 8, 7, 5), (3,6)

les racines de $g(x) = x^6 + x^3 + 1$ sont β, β^2, β^4, β^8, β^7, β^5. β racine primitive 9ième de l'unité $\beta = \alpha^7$.

Il ya 2 racines d'exposants consécutifs β, β^2,
Le poids minimum du code cyclique C de générateur $g(x)$ est au moins 3

codes BCH (Bose Chaudhuri Hocquemghen)

définition

Un code BCH est un code cyclique de **distance construite** δ est un code cyclique dont le générateur est le produit des polynômes minimaux de $\beta^r, \beta^{r+1}, \cdots, \beta^{r+\delta-2}$ pour un entier r donné

$r = 1$: BCH au sens strict

exemple

pour obtenir un code BCH de longueur 9 sur $\mathbb{F}_2$ de distance construite 4 : choisir $g(x) = (x^6 + x^3 + 1)(x^2 + x + 1)$
$g(x) = ppcm\{f_1(x)f_3(x)\}$

codes BCH (Bose Chaudhuri Hocquemghen)

théorème

Un code BCH de longueur n sur $\mathbb{F}_q$ et de distance construite δ a une distance minimale $d \geq \delta$ et une dimension $k \geq n - m(\delta - 1)$

REMARQUES

- le théorème donne une borne inférieure pour la distance minimale de C
- le théorème permet de trouver un code sur $\mathbb{F}_q$ corrigeant e erreurs pour n'importe quel e, il suffit de trouver un n tel qu'un diviseur de $x^n - 1$ satisfasse les conditions du théorème
- existence de techniques de codage et de décodage efficaces $\Rightarrow$ utilisations industrielles

codes Reed Solomon

définition

Un code de Reed Solomon (RS) sur $\mathbb{F}_q$ est un code BCH de longueur $n = q - 1$
(la longueur est le nombre d'èléments non nuls de $\mathbb{F}_q$))

- un code de Reed Solomon est un code cyclique de longueur $n = q - 1$ sur $\mathbb{F}_q$ de polynôme générateur
  $g(x) = (x - \alpha^r)(x - \alpha^{r+1}) \cdots (x - \alpha^{r+d-2})$
  où α est un élément primitif de $\mathbb{F}_q$.
- de dimension $k = n - d + 1$
- de distance minimale d (égale à la distance construite δ)

codes Reed Solomon : Exemple

$n = 3$, $q = 4$, $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ avec $f(x) = x^2 + x + 1$

si $d = 2$ alors $g(x) = x - \alpha$, et $k = 2$, le code C a 4^2mots

000	$1\alpha 0$	$\alpha^2 0 \alpha$	$\alpha^2 \alpha 1$
01α	$\alpha\alpha^2 0$	$10\alpha^2$	111
$0\alpha\alpha^2$	$\alpha^2 10$	$1\alpha^2\alpha$	$\alpha\alpha\alpha$
$0\alpha^2 1$	$\alpha 01$	$\alpha 1\alpha^2$	$\alpha^2\alpha^2\alpha^2$

codes Reed Solomon

REMARQUES

- la longueur est inférieure au nombre d'éléments du corps
- distance minimale
- à partir des codes RS sur $\mathbb{F}_q$ avec $q = p^m$ on peut construire des codes sur F_p avec une grande distance minimale
- codes adaptés pour la correction de paquets d'erreurs
- il existe de très bonnes méthodes de codage /décodage our ces codes

codes Reed Solomon : Image binaire Exemple

code Reed Solomon $C(3,2,2)$ sur $\mathbb{F}_4$

$\mathbb{F}_4$ espace vectoriel de dimension 2 sur $\mathbb{F}_2$ on peut construire un code $C(6,4,2)$ sur $\mathbb{F}_2$ appelé l'image binaire de $C(3,2,2)$ en utilisant la correspondance :

$$\begin{aligned} 0 &\Rightarrow 00 \\ 1 &\Rightarrow 10 \\ \alpha &\Rightarrow 01 \\ \alpha^2 &\Rightarrow 11 \end{aligned}$$

codes Reed Solomon : Image binaire Exemple

code Reed Solomon $C(3, 2, 2)$ sur $\mathbb{F}_4$

$C(6, 4, 2)$ sur $\mathbb{F}_2$

000000	100100	110001	110110
001001	011100	100011	101010
000111	111000	101101	010101
001110	010010	011011	111111

utilisation des codes dans des applications industrielles

Quelques exemples :

- Code de Hamming $(127, 120, 3)$ Minitel
- Transmission par satellites Reed Solomon $(255, 223, 33)$
- Disque Compact Reed Solomon raccourcis entrelacés $C_1(28, 24, 5)$ et $C_2(32, 28, 5)$ sur $\mathbb{F}_{2^8}$