Corps Finis et Codes Correcteurs d'erreurs

Baddou Mebarka Nariman
Encadreur:Mohammed Boussaid
Université Kasdi Merbah Ouargla 30000, Algerie
Département de Mathématiques
Option:Algébre et Géométrie
bnaritta@gmail.com

Résumé

Les codes correcteurs permettent de corriger une ou plusieurs erreurs dans un mot de code en ajoutant aux informations des symboles redondants, i.e. des symboles de contrôle. Différents codess correcteurs existent, mais dans ce document nous traiterons seulement les codes ReedMuller et les codes BCH.

Mots Clés: *Corps finis,polynôme sur corps finis* $F_p[X]$*,codage d'information,codes correcteurs d'erreurs*

1. Introduction

La théorie des codes est développée pour répondre aux problèmex de la correction des erreurs dans un systéme d'information. Lorsquon veut transmettre une information dun lieu A vers un lieu B, la première tâche consiste â transcrire le message en une suite de caractères dun alphabet adéquat. Cest ce quon appelle le (codage de linformation). Le principe de construction d'un code correcteurs d'erreurs systématique consiste ajouter aux mots constitués de m éléments d'information $a_1a_2\dots a_m$, où les a_i parcourent un corps fini $\mathbb{F}_q$, des élément (dits de contrôle) $a_{m+1}a_{m+2}\dots a_{m+k}$ déterminés par le biais d'une fonction (dite fonction de codage).

2. Préliminaires

Notation
$\mathbb{F}_p$: un corps fini à p éléments.

$C(n,k,d)$: un code linéaire C de longueur n, de dimension k et de distance minimale d.

G : Matrice génératrice de C.
Corps finis. On appelle corps fini tout corps dont le cardinal est fini. Soit K un corps fini; nous avons un homomorphisme d'anneaux canonique de $\mathbb{Z}$ dans K qui associe à tout entier n l'élémnt $n\cdot 1\in K$. Comme K est intgre, le noyau de ce dernier homomorphisme est de la forme $p\mathbb{Z}$, où p est un nombre premier. L'image de ce homomorphisme est formée par les éléments $0,1,\dots,p-1$; ainsi, ces éléments forment un sous-corps de K isomorphe à $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ (ceci signifie que K est de est de caractéristique $p>0$.

On peut voir K comme un espace vectoriel sur le corps $\mathbb{F}_p=\{0,1,\dots,p-1\}$ (par multiplication à gauche); si n désigne la dimension de K, alors K est isomorphe en tant qu'espace vectoriel $\mathbf{F}_p^n$. Ceci montre que K contient p^n éléments.

On peut montrer que deux corps qui ont le même cardinal p^n sont isomorphes; on note ce unique corps par $\mathbf{F}_{p^n}$.

Pour tout nombre premier p, et tout entier positif n, il existe un corps de cardinal p^n; on peut raliser ce dernier comme le corps de décomposition du polynôme $X^{p^n}-X\in\mathbb{F}_p[X]$.

2.1 Polynôme sur corps finis $F_p[X]$

Proposition
le polynôme $p=x^2+x+1$est irréductible sur le corps F_2
Preuve
il est clair $(P)=1et(P)=1modulo2$ .donc P n'a pas de racine dans F_2 il est donc irreductible sur F_2.
Exemple
On note,pour tout $p\in\mathbf{N}^*,\mathbf{F}_{p^n}$ le corps fini P^n éléments.On a notamment,pour tout P premier:$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$.
Proposition
Soit p premier,et $n\in\mathbf{N}_*$.Alors il existe un polynôme irréductible de $\mathbf{F}_p[X]$ de degré n.
F_4

1. On pose $Q=X^2+X+1$.Comme ,le degré de Q est de degré inférieur ou égal à 3 et qu'il n'a pas de racine dans $\mathbf{F}_2[X]$,alors Q est irrductible.Donc $\mathbf{F}_4=\mathbf{F}_2[X]/(Q)$.On a:$\mathbf{F}_4=0,1,X,X+1$.
2. $(1,X)$ engendre $\mathbf{F}_4$.On a:$X^2=X+1.(car-1=1)$
3. la loi additive du corps est:

+	1	X	X+1
1	0	X+1	X
X	x+1	0	1
X+1	x	1	0

4. La loi multiplicative du corps est:

×	X	X+1
X	X+1	1
X+1	1	X

3. Énoncé des resultats

3.1 Codes linéaires

- On dit que C est un code binaire si $A=\mathbf{F}_2=(0,1)$.
- Si **F** est un corps fini et C est un sous-espace vectoriel de dimension k de $\mathbf{F}^n$,alors C est dit un code linaire de longueur n et de dimension k qu'on note C(n,k).

1.La matrice génératrice
Une matrice gnratrice d'un code linaire C(n,k),note G,est une matrice d'ordre k dont les vecteur lignes forment une base de C(n,k).
Notons qu'il existe autant de matrices gnratrices pour un code linaire que de bases du sous espace C(n,k).
L'encodage de C(n,k) associ

$$G=\begin{pmatrix}g_1\\g_2\\\vdots\\g_k\end{pmatrix}$$

est l'aplication linaire

$$\phi:\mathbf{F}^k\longrightarrow C(n,k)\subset\mathbf{F}^n$$

dont la matrice associe,relativement la base canonique de F^k et la base $g_1,g_2,\dots,g_k$ de C(n,k),est la transpose de G.Tout message $u=(u_1,\dots,u_k)\in\mathbf{F}^k$ est cod par

$$\phi(u)=G^t.\begin{pmatrix}u_1\\u_2\\\vdots\\u_k\end{pmatrix}$$

L'application $\phi:F^k\longrightarrow C(n,k)$ est bijective car la matrice G est de rang maximum k.
2.La matrice de contrôle
Etant donn le code linaire $C=C(n,k)$ de matrice gnratrice G.Considrons l'orthogonal (suivant le produit scalaire usuel sur F^n) de C:

$$C^\perp=v\in V:v^tc=0:\forall c\in C$$

Lemme 1
Soit $C=C(n,k)$
- $C^\perp=C(n,n-k)$ (dit code dual de C).
- Si H est une matrice gnratrice de $C^\perp$alors

$$C=c\in V:H^tc=0$$

- Pour toutes matrices gnratrices G et H de C et $C^\perp$ respectivement,on a $H^t.G=0$.

Preuve
Le sous espace orthogonal de l'espace ligne de la matrice H,qu'on applle l'espace nul de la matrice H est exactement le code C.En d'autre terme,on peut crire:

$$C=c\in V:H^tc=0$$

Il est clair qu'on a la relation suivante :

$$H^tc=0$$

.

La matrice H est appelle la matrice de contrôle du code C. ■

References

[1] Khalifa ZIZI, Groups Anneaux Corps, Office des publications Universitaires:01-2016,page 447-489.
[2] GHECHAMI NAANAA . tude comparative des codes classiques . Thèse de magister luniversité de batna ,2001 .