UNIVERSITE KASDI MERBAH
OUARGLA
Faculté des Mathématiques et des Sciences
de la Matière

N° d'ordre :
N° de série :

DEPARTEMENT DE
MATHEMATIQUES

MASTER

Spécialité : Mathématiques

Option : Algébre et Géométrie

Par : Baddou Mebarka Nariman

Théme

Corps Finis Et Codes Correcteurs Des Erreurs

Soutenu publiquement le : ../06/2018

Devant le jury composé de :

Mr.Mohammed.A BAHAYOU	M.A. Université KASDI Merbah- Ouargla	Président
Mr.Yacine GUERBOUSSA	M.A. Université KASDI Merbah- Ouargla	Examinateur
Mr.Mohammed.T BENMOUSSA	M.A. Université KASDI Merbah- Ouargla	Examinateur
Mr. Mohammed BOUSSAID	M.A. Université KASDI Merbah- Ouargla	Rapporteur

Dédicaces

je dédie ce modeste travail à ma chère mère,
A mon cher père qui m'ont toujours soutenu, qui m'ont aide à affronter les difficultés,
Á mon cher Mari, Á mes frères m.Said Loubna chahinaz Mahdi. À mon neveu, Iyad,
à A toute ma famille. et à mes amis,
à mes collègues, qui ont voyagé ensemble pour atteindre le chemin du succès .
A tous mes enseignants pour leurs utiles conseils, leurs partience, leur persévérance. et à toutes les personnes que je porte dans mon cœur de près et de loin.

Remerciement

Je remercie vivement mon encadreur, **Mr : Mohammed BOUSSAID**, sur sa proposition ce sujet et son organisation nous ont permis de surmonter de nombreuses difficultés liées à ce travail.

Merci également à tous ceux qui ont contribué à notre formation spirituelle. Notre gratitude s'adresse également à tous ceux qui, de loin ou de prés, ont participé à la réalisation de ce travail. Nous tenons aussi à remercier toute l'équipe pédagogique pour nous avoir transmis leur savoir tout au long de notre cycle d'étude.

Je remercie sincèrement les membres du jury et également les membres du département de Mathématique et Informatique de m'avoir permis de travailler dans de bonnes conditions pendant la réalisation de mon travail.

Table des matières

Introduction

La théorie des codes est développée pour répondre aux problèmex de la correction des erreurs dans un systéme d'information. Lorsqu'on veut transmettre une information d'un lieu A vers un lieu B, la première tâche consiste â transcrire le message en une suite de caractères d'un alphabet adéquat. C'est ce qu'on appelle le (codage de l'information). Le principe de construction d'un code correcteurs d'erreurs systématique consiste à 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).

- Dons le chapitre 1 on rappelle quelques notions, concerne les corps finis. On démontre enparticulier le théorème de wedderburn qui dit que tout corps fini est commutatif et le polynôme sur corps finis à p^m éléments pour un nombre premire p.
- Le chapitre 2 défini la notion de code linéaire, matrice génératrice, matrice de contrôle, code de Hamming.
- Le chapitre 3 On aborde celle du décodage par tableau standard et de décodage par la méthode syndrome. et donne quelques exemples : code de Hamming, code B.C.H, code de reed-muller

Chapitre 1

CORPS FINIS

1.1 Définitions et Premières propriétés

1.1.1 Définition du corps $\mathbb{F}_p$

[1] On ne revient pas sur la construction de corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (pour p premier). Ce corps est fini de cardinal **p** et de caractéristique **p** également.

1.1.2 Proposition(unicité du corps $\mathbb{F}_p$)

Si p est un nombre premier,$\mathbb{Z}/p\mathbb{Z}$ est un corps. De plus, c'est l'unique corps de cardinal p, à isomorphisme de corps prés.

Preuve : Soit K un corps de cardinal p, alors $(k, +)$ est un groupe de cardinal p donc est cyclique. Notons 1_k le neutre multiplicatif, qui engendre donc $(K, +)$. Si $a, b \in K$, notons $a = a'.1_k = (1_k + \cdots + 1_k)(a' fois)$ et $b = b'.1_k$.Alors $ab = (a'.1_k) \times (b'.1_k) = (a'b').1$ (Par distributivité). La loi multiplicative est donc uniquement déterminée. [1]

1.1.3 Proposition(que tout corps est un sur corps de $\mathbb{Q}$ ou $\mathbb{F}_p$)

Pour tout corps fini K, il existe p premier tel que F_p s'injecte dans K via un morphisme de corps. **Preuve :** Il suffit de considérer le sous corps engendré par le neutre multiplicatif, et d'utiliser la primalité de la caractéristique. [1]

1.2 Caractéristique.Sous corps premier

[2] Soit K un corps commutatif. Considérrons le morphisme d'anneau

$$\phi = \begin{cases} \mathbb{Z} \longrightarrow K \\ m \longrightarrow m.1 = 1 + 1 + \cdots + 1(mfois) \end{cases}$$

Deux situations peuvent se présenter

- $\ker \phi = 0$

ϕ est alors injectif et peut être étandue à $\mathbb{Q}$ par $\phi(m/n) = m.1/n.1$, dans ce cas on confond $\mathbb{Q}$ et $\phi(\mathbb{Q})$ et on considére $\mathbb{Q}$ comme un sous corps de K.

- $\ker\phi = p\mathbb{Z}$

L'entier p est alors un nombre premier, sinon on aurait $p.1 = (m.1)(n.1) = 0 \Rightarrow (m.1 = 0)$ ou $(n.1 = 0)$ ce qui est le plus petit entier positif vérifiant cette propriété. On a alors
$\phi(x) = \phi(y) \Leftrightarrow x - y \in p\mathbb{Z} \Leftrightarrow x \equiv y \bmod p$ L'application $\phi = \begin{cases} \mathbb{Z}/p\mathbb{Z} \longrightarrow k \\ \bar{m} \longrightarrow m.1 \end{cases}$ est alors injective et $\mathbb{Z}/p\mathbb{Z}$ peut être considére comme un sous coprs de K.
Le nombre p qui est nul ou est premier est appelé **Caractéristique** du corps K. Si $p = 0$, $\mathbb{Q}$ est appelé sous corps premier de K. Si p est premier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est également appelé sous corps premier de K.
le sous corps premier est dans les deux cas le plus petit corps contenu dans K.
Un corps fini a donc une caractéristique $p > 0$ et contient $\mathbb{F}_p$ comme sous corps premier.

1.3 Extension de corps

1.3.1 Définition

[3] Si K et L sont des corps, on appelle morphisme de corps tout morphisme d'anneaux $f : K \to L$. Un tel morphisme est injectif et aussi appellé extension de K. Le degré de l'extension, noté $[L : K]$ est la dimension de L. comme espace vectoriel sur K.

1.3.2 Proposition

a) Si K est un corps de caractéristique nulle, alors il existe une unique extension $f : \mathbb{Q} \to K$.
b) Si K est un corps de caractéristique $p > 0$, alors il existe une unique extension $f : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to K$. [3]

1.3.3 Proposition

Soient $f : K \to L$ une extension de K et
$g : L \to L'$ une extension de L alors :

$$[L' : K] = [L' : L][L : K].$$

[L :K] est le degré de L sur K ($K \subseteq L$). [3]

1.3.4 théorème

Soit $f(X)$ un polynôme irréductible sur $\mathbb{F}_p$,de degré n. L'anneau quotient $K = \mathbb{F}_p[X]/(f(X))$ est un corps fini de cardinal p^n.

Démonstration :
le polynôme $(f(X))$ étant irréductible, K est bien un corps. Soit $(g(X))$ un polynôme de $\mathbb{F}_p[X]$ et $r(X)$ le reste de la division de ce polynôme par $f(X)$
Posons :$x = \bar{X} = X + (f(X))$. On a $g(\bar{X}) = r(\bar{X}) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$,$a_i \in \mathbb{F}_p$,$i = 0, 1, \ldots, n-1$ où $r(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$. K est un espace vectoriel sur $\mathbb{F}_p$ et on vérifie que $(1, x, x^2, \ldots, x^{n-1})$ est une base de cet espace vectoriel qui est donc de dimension n sur $\mathbb{F}_p$ ce qui permet d'obtenir p^n éléments distincts. Un raisonnement analogue montre que

tout corps fini de caractéristique p a un cardinal p^n pour un entier n. [2]

Remarque

Soit K un corps et $f(X)$ un polynôme irréductible sur K de degré > 1, il existe un plus petit corps L(à un isomorphisme prés), extension de K, dans lequel $f(X)$ admet un zéro.Définissons $L = K[X]/(f(X))$ et on pose $x = \bar{X} = X + (f(X))$, on a $f(X) = 0$. Un corps vérifiant cette propriété est appelé corps de rupture de $f(X)$. En répétant cette opération.On obtient un corps extension de K contenant toutes les racines de $f(X)$. Ce corps est aussi unique à isomorphisme prés.

1.3.5 Définition

[4] corps finis K est de caractéristique $p > 1$. Il peut être vu comme extension de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ via le morphisme $\mathbb{F}_p \longrightarrow K$, $\bar{x} \longrightarrow x.1_k$. En particulier c'est un $\mathbb{F}_p$ espace vectoriel de dimension finie donc le cardinal de K est une puissance de p. En sens inverse,on a :

1.3.6 théorème

Soit $q = p^n$ avec $n \in \mathbb{N}^*$. Alors il existe un corps de cardinal q, unique à isomorphisme prés. C'est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$.On note ce corps $\mathbb{F}_q$

Démonstration : Soit K le corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^q - X$. On note que l'ensemble K' des racines dans K de $X^q - X$ est déjà un corps, en vertu de l'identité $(x + y)^{p^n} = x^{p^n} + y^{p^n}$, qui se montre par récurrence sur n en utilisant le fait que tous les coefficients binomiaux C_p^k sont divisibles par p pour $0 < k < p$. Par définition du corps de décomposition, on a $K = K'$. D'autre part la dérivée de $X^q - X$ est $X^{q-1} - 1 = -1$, donc toutes les racines sont simples et il y en a donc q. Finalement K est bien un corps de cardinal q. [4]

Par exmple

On a $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$, $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1)$

Remarque : Toute algèbre à division finie est un corps (théorème de Wedderburn), autrement dit il n'y a pas de "corps non commutatifs" finis.

1.3.7 théorème :(Wedderburn)

[5] tout corps fini est commutatif

preuve :

soit F un corps fini, Z son centre. Z est un sous-corps commutatif et F est un espace vectoriel sur Z. Comme F est fini, il possède un nombre fini de générateurs donc il est de dimension finie. Soit $|Z| = q \geq 2$ donc $|F| = q^n$. On va raisonner par l'absurde en supposant que F n'est pas commutatif donc $Z \neq F$ et par suite $n > 1$. Faisons opérer le groupe multiplicatif F^* sur lui-même par ses automorphismes intérieurs. Soit $x \in F^*$ et $C(x) = y \in F : yx = xy$ le commutant de x. C'est un corps (non nécessairement commutatif) et par suite un espace vectoriel sur Z donc $|C(x)| = q^d$. Comme $C^*(x)$ est un sous-groupe de F^* alors $q^d - 1$ divise $q^n - 1$.

1.4 POLYNÔME SUR CORPS FINIS $F_p[X]$

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'élément $n \cdot 1 \in K$. Comme K est intègre, 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 $0, 1, \ldots, p-1$; 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 $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ (par multiplication à gauche) ; si n désigne la dimension de K, alors K est isomorphe en tant qu'espace vectoriel à $\mathbf{F}_p^n$. 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 réaliser ce dernier comme le corps de décomposition du polynôme $X^{p^n} - X \in \mathbb{F}_p[X]$.

1.4.1 proposition

le polynôme $P(X) = X^2 + X + 1$ est irréductible sur le corps $\mathbb{F}_2$.

preuve :

il est clair $P(0) = 1$ *et* $P(1) = 1 modulo 2$. donc P n'a pas de racine dans $\mathbb{F}_2$ il est donc irreductible sur $\mathbb{F}_2$. [5]

1.4.2 théorème

le corps des racine du polynôme $P(X) = X^2 + X + 1$sur F_2 est donné par l'extension algébrique simple $F_2[\alpha]$ où $[\alpha]^2 = [\alpha] + 1$. de faÇon plus préécise

$$F_2[\alpha] = a + b\alpha : a, b \in \mathbb{F}_2$$

Ce corps de caractéristique 2, a 4 éléments est donc isomorphe *à* $\mathbb{F}_4$. En particulier on a

$$x^2 + x + 1 = (x - \alpha)(x - 1 - \alpha).$$

α engendre le groupe multiplicatif des élément non nuls de$\mathbb{F}_2^2$. On les relations

$$\alpha^2 = \alpha + 1, \alpha^3 = \alpha + 1 + \alpha = 1.$$

preuve :

nous avons montré que P(X) est irreductible sur $\mathbb{F}_2$. Donc il possède un corps de racines. Soit α une racine de P donc $\alpha^2+\alpha+1 = 0$ ou encore $\alpha^2 = -\alpha-1 = \alpha+1$. Alors $(X-\alpha)(X-1-\alpha) = X^2 - (1 + \alpha + \alpha)X + \alpha^2 + \alpha = X^2 - X - 1 = X^2 + X + 1$ En outre

$$\alpha^2 = \alpha + 1, \alpha^3 = \alpha^2 + \alpha = 2\alpha + 1 = 1$$

[5]

	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$\alpha+1$	1
$1+\alpha$	$1+\alpha$	1	α

TaB. 1.1 -Table du groupe multiplication $\mathbb{F}_{2^2}^*$

1.4.3 proposition

les polynômes $P_1(X) = X^3 + X + 1$ et $P_2(X) = X^3 + X^2 + 1$ sont irréductibles sur le corps $\mathbb{F}_2$.

preuve :

en effet on a : $P_1(0) = 1$, $P_1(1) = 1$; $P_2(0) = 1$, $P_2(1) = 1$. n'ayant pas des racines dans $\mathbb{F}_2$, est irrecductible sur $\mathbb{F}_2$ puisque dans le cas contraire, il est le produit de deux polynômes l'un de degré 1 et l'autre de degré 2. [5]

1.5 Exemples

[1]On note,pour tout $p \in \mathbb{N}^*, \mathbb{F}_{p^n}$ le corps fini à p^n éléments. On a notamment, pour tout P premier :$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1.5.1 $\mathbb{F}_4$

1. On pose $Q(X) = X^2 + X + 1$.Comme, le degré de $Q(X)$ est de degré inférieur ou égal à 3 et qu'il n'a pas de racine dans $\mathbb{F}_2[X]$, alors Q(X) est irréductible.
   Donc $\mathbb{F}_4 = \mathbb{F}_2[X]/ < Q(X) >$. On a :$\mathbb{F}_4 = 0, 1, X, X + 1$.

2. $1, X$ engendre $\mathbb{F}_4$. 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

1.5.2 $\mathbb{F}_8$

1. On pose $Q(X) = X^3 + X + 1$. Encore une fois, le degré de Q(X) est inférieur ou égal à 3 est $Q(X)$ n'admet pas de racines dans $\mathbb{F}_2$. Donc $\mathbb{F}_8 = \mathbb{F}_2[X]/ < Q(X) >$.

2. Pour simplifer le calcul, regardons les multiplications des générateurs du corps :

1	X	X^2
X	X^2	X+1
X^2	X+1	X

3. Calculons les itérés de X : $X \longrightarrow X^2 \longrightarrow X+1 \longrightarrow X^2+X \longrightarrow X^2+X+1 \longrightarrow X^2+1 \longrightarrow 1$.On savait déjà que $\mathbb{F}_8^*$ était cyclique. Et X en est un générateur (en fait,ils sont tous générateurs car 7 est premier)

4. Regardons la loi de corps :

1	X	X^2	$X+1$	X^2+X	X^2+X+1	X^2+1
X	X^2	$X+1$	X^2+x	X^2+X+1	X^2+1	1
X^2	$X+1$	X^2+X	X^2+X+1	X^2+1	1	X
$X+1$	X^2+X	X^2+X+1	X^2+1	1	X	X^2
X^2+X	X^2+X+1	X^2+1	1	X	X^2	$X+1$
X^2+X+1	X^2+1	1	X	X^2	$X+1$	X^2+X
X^2+1	1	X	X^2	$X+1$	X^2+X	X^2+X+1

5. On remarque que $\mathbb{F}_4$ ne s'injecte pas dans $\mathbb{F}_8$. En effet, il n'y a pas de sous-corps de cardinal 4 dans $\mathbb{F}_8$, car tout élément engendre multiplicativement $\mathbb{F}_8^*$.

Chapitre 2

Codes correcteurs d'erreurs

2.1 Codes linéaires

Cette famille de codes est développeé par Mac Williams et Sloane dans les années 50.

Définition 1

[6] • Soit A un ensemble fini, dit alphabet. L'ansemble des mots de longueur finie formés avec les symboles de A, muni de la loi de composition interne "concaténation" est un monoïde libre, noté $\bar{A}$. L'élément neutre de cette loi est le mot vide.

• Un code C sur A est un sous ensemble de $\bar{A}$.Les éléments c de C sont dits "mots codes"

• On dit que C est un code binaire si $A = \mathbb{F}_2 = (0, 1)$.

• Si tous les mots codes de C sont de même longueur, on dit que C est un code en bloc. Dans le cas contraire C est un code à longueur variable.

Définition 2

Si $\mathbb{F}$ est un corps fini et C est un sous-espace vectoriel de dimension k de $\mathbb{F}^n$, alors C est dit un code linéaire de longueur n et de dimension k qu'on note C(n,k).[6]

2.1.1 Matrice génératrice

Définition 1

Si le message est $u = u_1u_2 \dots u_k$ quel est le mot de code correspondant ? D'abord $x_1 = u_1, x_2 = u_2, \dots x_k = u_k$ on encore

$$\begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = I_k \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$$

[5]

Proposition 2

La matrice génératrice d'un code linéaire a pour lignes une base du sous-espace vectoriel formé par les mots de code. Réciproquement si C est un sous-espace de $\mathbb{F}^n$ admettant $g_1, g_2, \dots, g_k$ pour base,la matrice ayant pour lignes les composantes des g_i est la matrice génératrice d'un code linéaire de dimension k.

Preuve :

Par définition de G,x est un mot de code si et seulement si

$$x = u_1g_1 + u_2g_2 + \cdots + u_kg_k$$

.

Les vecteurs (g_i) engendrent donc le code C mais comme le code est de dimension k, ces vecteurs forment une base de C. La réciproque est immédiate. Etant donné un code linéaire C(n,k) sur le corps F. Soient $g_1, g_2, \dots, g_k$ une base de C(n,k). Alors tout élément c de C(n,k) est de la forme $c = u_1.g_1 + u_2.g_2 + \cdots + u_k.g_k$.

En posant

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

on obtient $c = u.G$ où $u = (u_1, u_2, \dots, u_k)$.

Proposition 3

Soit C(n,k) un code linéaire dont $g_1, g_2, \dots, g_k$ est une base de C(n,k), alors tout éléments de

C(n,k) s'écrit sous la forme

$$C = c : c = u.G, u \in \mathbb{F}^k$$

où

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

est une matrice de type $k \times n$.

Définition 4

Une matrice génératrice d'un code linéaire C(n,k), notée 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 génératrices pour un code linéaire que de base du sous espace C(n,k).

L'encodage de C(n,k) associé à

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

est l'aplication linéaire

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

dont la matrice associée,relativement à la base canonique de F^k et la base $g_1, g_2, \ldots, g_k$ de C(n,k), est la transposée de G. Tout message $u = (u_1, \ldots, u_k) \in \mathbf{F}^k$ est codé 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.

2.1.2 Matrice de contrôle

Définition 1

Soit H une matrice à éléments dans un corps F_q à $n-k$ lignes et n colonnes, de rang $n-k$ c'est-à-dire que les $r = n-k$ lignes sont indépendantes.On appelle code linéaire de contrôle de parité H, l'ensemble C des vecteurs lignes $x = (x_1, x_2, \ldots, x_n)$ de $\mathbb{F}_q^n$ qui vérifient l'équation

$$H^t x = 0$$

Définition 2

On dit qu'un code linéaire est sous forme systématique lorsque le mot d'information u se trouve dans des coordonnées préfixées du mot de code correspondant. En particulier lorsque ces positions préfixées sont les k premières, nous dirons qu'il s'agit d'un codage systématique standard.

$$x_1 = u_1, x_2 = u_2, \ldots, x_k = u_k$$

suivie de n-k symboles de contrôle

$$x_{k+1} x_{k+2} \ldots x_n$$

$$x = \underbrace{x_1 x_2 \ldots x_k}_{symboles\ \ du\ \ message} \quad \underbrace{x_{k+1} x_{k+2} \ldots x_n}_{symboles\ \ de\ \ contrle}$$

la matrice de contrôle du code est alors donnée sous la forme

$$H = [A | I_{n-k}]$$

A est une matrice à k colonnes et $n-k$ lignes tandis que I_{n-k} est la matrice carrée unité d'ordre $n-k$. Les opérations sont effectuées dans le corps fini $\mathbb{F}_q$.

Définition 3

Etant donné le code linéaire $C = C(n, k)$ de matrice génératrice G. Considérons l'orthogonal (suivant le produit scalaire usuel sur F^n) de C :

$$C^{\perp} = v \in V : v^t c = 0 : \forall c \in C$$

Lemme 4

Soit $C = C(n, k)$

• $C^{\perp} = C(n, n-k)$ (dit code dual de C).

• Si H est une matrice génératrice de $C^{\perp}$alors

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

• Pour toutes matrices génératrices 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 appèlle l'espace nul de la matrice H est exactement le code C. En d'autre terme,on peut écrire :

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

Il est clair qu'on a la relation suivante :

$$H^t c = 0$$

La matrice H est appellée la matrice de contrôle du code C. [6]

Exemple de Code

Il est défini par la matrice de contrôle de parité

$$H = \begin{bmatrix} 011|100 \\ 101|010 \\ 110|001 \end{bmatrix}$$

(la barre verticale est seulement symbolique) à termes dans $\mathbb{F}_2$ c'est un code avec $k = 3$ et $n = 6$.Pour ce code la matrice A est donnée par

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Un message $u = u_1u_2u_3$ est encodé en le mot de code $x = x_1x_2x_3x_4x_5x_6$ de telle sorte que

$$x_2 + x_3 + x_4 = 0 \quad (1)$$

$$x_1 + x_3 + x_5 = 0 \quad (2)$$

$$x_1 + x_2 + x_6 = 0 \quad (3)$$

Par exemple si le message d'information est $u = 011$,alors $x_1 = u_1 = 0, x_2 = u_2 = 1, x_3 = u_3 = 1$ et les symboles de contrôle de parité sont

$$x_4 = -x_2 - x_3 = -1 - 1 = -2 = 0$$

$$x_5 = -x_1 - x_3 = -1 = 1$$

$$x_6 = -x_1 - x_2 = -1 = 1$$

donc le mot de code correspondant est $x = 011011$. Les équations $(1), (2), (3)$, sont appelées (les équations de contrôle de parité) ou tout simplement équations de parité du code. L'équation (1) exprime que la somme des $2me, 3me$ et $4me$ symboles est nulle dans $\mathbb{F}_2$ ou encore que la somme dans $\mathbb{Z}$ est un nombre pair d'où le nom de ces équations.Comme chacun des symboles du message est 0 ou 1, et que le message comporte 3 symboles, il y a donc 2^3 messages et par suite 8 mots de codes.

2.2 Codes de Hamming

Les codes de hamming sont des codes linéaires. Ils sont caractérisés par l'aisance de codage et de décodage. Ils ont été introduits par Golay en 1949, et par Hamming en 1950.
Nous donnons une présentation succinte,dans ce qui suit, les codes de Hamming binaires (tous les résultats sont généralisables au cas des corps finis quelconques).

2.2.1 Définition

soit m un entier ≥ 2.Sur le corps F_{q^m}, on introduit la relation d'équivalence

$$a \equiv b \Longleftrightarrow \exists \lambda \in F_q^*, b \equiv \lambda a$$

.
On appelle code Hamming la matrice de contrôle H a n colonnes

$$n = \frac{q^m - 1}{q - 1}$$

et m lignes construites de la façon suivante : on choisit dans chacune des n classes d'équivalence un représentant constitue la colonne de H. Dans le cas où $q = 2$,on a donc $n = 2^m - 1$ et comme $m = n - k$ on a $k = 2^m - m - 1$. Autrement dit un code de Hamming binaire a pour paramètres $[2^m - 1, 2^m - m - 1]$. La relation d'équivalence est seulement la relation d'égalité. Donc les classes d'équivalence sont réduites à un seul élément non nul. [5]

2.2.2 Définition

Le code de Hamming à m bits de contrôle, noté Ham(m) est le code linéaire de longueur $n = 2^m - 1$, dont la matrice de contrôle $H_m = (h_1, h_2, \ldots, h_n)$ est caractérisée par :
"le i^{ime} vecteur colonne h_i est la représentation binaire de l'entier naturel i dans $\mathbb{F}_2$.
Autrement dit $Ham(m)$ est un $C(2^m - 1, 2^m - m - 1)$ et avec :

$$H_m = \begin{pmatrix} 00\ldots1 \\ \ldots\ldots \\ \ldots\ldots \\ \ldots\ldots \\ \ldots\ldots \\ 01\ldots1 \\ 10\ldots1 \end{pmatrix}$$

Exemple

On prend $m = 3$ donc $n = 2^3 - 1 = 7, k = 2^3 - 3 - 1 = 4$. On a donc un code de Hamming $C(7, 4)$.La matrice de contrôle de parité est

$$H = \begin{bmatrix} 0111100 \\ 1011010 \\ 1101001 \end{bmatrix}$$

à coefficients dans $\mathbb{F}_2$. C'est une matrice à $m = 3$ lignes et $n = 7$ colonnes donc $k = 2^3-3-1 = 4$. Il y a 2^4 mots de codes $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ qui satisfont les équations

$$x_2 + x_3 + x_4 + x_5 = 0 \quad (1)$$

$$x_1 + x_3 + x_4 + x_6 = 0 \quad (2)$$

$$x_1 + x_2 + x_4 + x_7 = 0 \quad (3)$$

ou encore

$$-x_5 = x_2 + x_3 + x_4$$

$$-x_6 = x_1 + x_3 + x_4$$

$$-x_7 = x_1 + x_2 + x_4$$

En général les colonnes sont disposées de façon que la i^{me} colonne coïncide avec le développement binaire de i.Alors la matrice de contrôle se présente sous la forme H'

$$H' = (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7)$$

$$= \begin{pmatrix} 0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,1\,0\,0\,1\,1 \\ 1\,0\,1\,0\,1\,0\,1 \end{pmatrix}$$

Cependant nous verrons dans le paragraphe suivant que les codes de Hamming sont des codes cycliques. On préférera alors la matrice de contrôle H" donnée par

$$H'' = \begin{pmatrix} 1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,0\,0\,1\,1 \\ 0\,0\,1\,1\,1\,0\,1 \end{pmatrix}$$

Chapitre 3

Décodage et Correction des erreurs

3.1 Distance de Hamming

Soit u un message qui a été encodé en un mot de code x. Après transmission par le canal on a reçu un message $T(x) = x^*$. On suppose que le canal induit une erreur qu'on symbolise par un vecteur d'erreur $e = (e_1, e_2, \ldots, e_n)$ de sort que $x^* = x + e$. Le rôle du décodeur est de trouver u et celui-ci est connu dès que $x = x^* - e$ est connu.
Malheureusement e n'est jamais connu. Par suite la stratégie du décodeur est de supposer que c'est la moindre erreur qui est commise. On dit aussi qu'il s'agit du décodage par vraisemblance maximale. Cela revient à faire l'hypothèse que chaque mot reçu $x^* \in \mathbb{F}_q^n$, le mot de code $D(x^*) = x^* - e$ est l'un des mots de code le plus proche de x^*.
Il nous faut mathématiser cette notion de proximité. Ce sera avec l'introduction de la distance de Hamming.

3.1.1 Définition

Soit A un alphabet quelconque. Etant donné deux éléments quelconques de A^n, $x = (x_i), \quad i = 1 \ldots nety = (y_i), \quad i = 1 \ldots n$,où $x_i, y_i \in A$ pour tout i, on appelle distance de Hamming entre

ces deux éléments, le nombre entier noté $d(x, y)$ égal au nombre de d'indices i tels que $x_i \neq y_i$. On a donc

$$0 \leqslant d(x, y) \leqslant n.$$

3.1.2 Proposition

l'application distance de Hamming d est bien une distance sur A^n c'est-à-dire vérifie les propriétes

$$\forall (x, y) \in A^n \times A^n, d(x, y) \geqslant 0, d(x, y) = 0 \Leftrightarrow x = y$$

$$\forall (x, y) \in A^n \times A^n, d(x, y) = d(y, x)$$

$$\forall (x, y, z) \in A^N \times A^n, d(x, y) \leqslant d(x, z) + d(z, y)$$

Preuve :

La première ainsi que la deuxième propriété sont évidentes. Pour tout i, si nous posons $d_i(x_i, y_i) =$ 0 ou1 suivant que $x_i = y_i$ ou $x_i \neq y_i$, on voit que $d(x, y) = d_1(x_1, y_1) + d_2(x_2, y_2) + \cdots + d_n(x_n, y_n)$ (somme dans $\mathbb{N}$). Or pour tout i, on a $d_i(x_i, y_i) \leq d_i(x_i, z_i) + d_i(z_i, y_i)$. En effet si $x_i = y_i$ cette inégalité devient évidente. Si $x_i \neq y_i$, on a nécessairement $x_i \neq z_i$ ou $y_i \neq z_i$ donc le second membre est ≥ 1 et l'inégalité est vérifiée. En faisant la somme de ces n inégalités.

3.1.3 Définition

Nous avons associé à un code C deux paramètres k et n, le premier est le nombre de symboles d'un message d'information. On appelle distance du code, la distance la plus petite entre les éléments de C :

$$d = mind(x, y), \quad x \neq y.$$

Nous dirons qu'il s'agit d'un code type [n,k,d].

3.1.4 Définition

Soit $A = \mathbb{F}_q$. On appelle poids d'un message $x \in A^n$, le nombre de coordonnées non nulles de x, qui est noté $w(x)$(w est l'abréviation du mot anglais weight qui signifie poids)

3.1.5 Proposition

Soit $A = \mathbb{F}_q$. Alors pour tout x et tout y éléments de A^n, la distance de Hamming de x et y est égale au poids de $x - y$(aussi bien que $y - x$) :

$$d(x, y) = w(x - y) = w(y - x).$$

Preuve :
En effet, si $x = (x_i), \quad i = 1 \dots n$ et $y = (y_i), \quad i = 1 \dots n$ donc $x - y = (x_i - y_i), i = 1 \dots n$. Alors $x_i \neq y_i$ si et seulement si $x_i - y_i \neq 0$(resp.$y_i - x_i \neq 0$) d'où notre assertion.

3.2 Décodage par le tableau standard

3.2.1 Théorème

Soit $C \subset \mathbb{F}_q^n$ un code linéaire de dimension k.

1. La relation S définie sur $\mathbb{F}_q^n$ par

$$xSy \Leftrightarrow x - y \in C$$

est une relation d'équivalence.

2. La classe d'équivalence du message x, $\Gamma(x)$ est formé par l'ensemble des messages $y = x + z : z \in C$. En particulier la classe de 0 est formée par l'ensemble C des mots de code.

3. Il y a $q^r (r = n - k)$ classe d'équivalence.

Preuve :

Comme $0 \in C$, La relation est réflexive. Si $x - y \in C$ alors C étant un espace vectoriel $-(x - y) = y - x \in C$ donc S est symétrique.Supposons $x - y \in C$ et $y - z \in C$ alors C étant un espace vectoriel, $(x - y) + (y - z) = x - z \in C$ donc S est un relation transitive. S est bien relation d'équivalence.

x est équivalent à 0 si et seulement $x = x - 0 \in C$ autrement dit si seulement si $x \in C$:la classe de 0 est l'ensemble des éléments du code. D'autre part y est équivalent à x si et seulement si $y - x \in C$ ou encore si et seulement si $x - y \in C$ donc si et seulement s'il existe $z \in C$tel que $y - x = z \Leftrightarrow y = x + z$: la classe de x est l'ensemble des mots de la forme $x + z$ où $z \in C$.

Toutes les classe d'équivalences ont le même nombre d'éléments égal au nombre de mots de code q^k. Comme le cardinal de l'ensemble des messages possibles est 2^n, il y a donc $q^n/2^k = q^r$ classe d'équivalence.

Methode de décodage :

Soit x un message, $\alpha = x + z$ un élément de la classe $\Gamma(x)$ avec $z \in C$. On a

$$d(x, z) = w(x - z) = w(\alpha)$$

Par conséquent,détecter le mot de code le plus proche de x revient à chercher dans sa classe celui qui a le poide le plus petit α , le mot de code est alors $\alpha - x$ (si $q = 2$ c'est aussi $x + \alpha$). Par conséquent pour faire le décodage, il faut déterminer les classe d'équivalence.Une fois, repéré dans la classe de x l'élément α de plus faible poids (s'il y a plusieurs, on prend un au hasard), il suffit de faire la soustraction $\alpha - x$(ou simplement l'addition si $q = 2$).

Le tableau standard

On peut rendre cette méthode plus mécanique en établissant le tableau de décodage appelé le tableau standard.

1. On écrit dans la prmière ligne du tableau la classe de 0 donc l'ensemble des mots de code en commençant par 0.

2. On cherche un message de poids 1 qui n'est pas un motde code qu'on écrit au début de la $2me$ ligne sous 0. On écrit la classe de cet élément dans les cases suivantes de la $2me$ en ajoutant à cet élément les éléments de code dans les cases correspondantes dans l'ordre choisi dans la première ligne.

3. Si le tableau n'est pas rempli, on choisit un message de plus petit poids parmi ceux qui ne sont pas déjà inscrits dans le tableau, qu'on écrit à gauche dans la ligne suivante qui va être remplie par les sommes de cet élément avec respectivement chaque élément du code en respectant l'ordre.

4. On continue ainsi jusqu'à épuiser tous les messages.

5. On aboutira ainsi à un tableau à 2^r lignes

Lecteure du tableau de décodage

On observera que les classes d'équivalence ont été énumérées suivant les lignes avec à gauche l'élément de plus faible poids. Soit x un message.

1. Si ce message se trouve dans la première ligne du tableau c'est un mot de code. On prend $D(x) = x$. Si ce n'est pas le cas, x est un message erroné. Il faut chercher $D(x)$ en passant à 2.

2. On cherche la ligne c'est-à-dire la classe qui contient x. Alors le mot de code $D(x)$ est le mot de code qui se trouve dans la même colonne. Il faut observer que ce mot de code s'obtien en retranchant à x le mot de plus petit poids qui se trouve dans la même ligne (aussi bien en ajoutant ce message si $q = 2$).

3.3 Décodage par la méthode du syndrome

3.3.1 Définition

Soit C un code linéaire dont la matrice de contrôle de parité est une matrice H à $r = n - k$ lignes et n colonnes. Elle détermine une application linéaire unique de A^n dans A^r qu'on note encore H. Pour tout message $x \in A^n$, on appelle syndrome de x l'image de x par H. Il est noté $s(x)$:

$$x = (x_1, x_2, \ldots, x_n)s(x) = H^t x.$$

3.3.2 Théorème

1. Le syndrome de la somme de deux message est la somme de leurs syndrome.
2. Le syndrome d'un message est de longueur $r = n - k$.
3. Il y a q^r syndrome différents.
4. Le syndrome d'un message est nul si et seulement si ce message est un mot de code.
5. Deux message x et y ont le même syndrome si et seulement si ils sont équivalents. En particulier si $x^* = x + e$, on a $s(x^* = s(e))$. L'erreur et le message erroné ont le même syndrome.
6. Pour un code binaire i.e $q = 2$, le syndrome d'un message $x = x_1 x_2 \ldots x_n$ est la somme des colonnes de H dont les numéros sont les indices des bits a_p égal à 1. En particulier, les colonnes de H sont tous les syndromes des messages de poids 1, les sommes deux à

deux des colonnes de cette matrice sont tous les syndromes des messages de poids 2, etc aux indices des symboles erronés.

Preuve :

Par définition $s(x)$ est l'image de x par l'application linéaire h de $\mathbb{F}_q^n$ dans $\mathbb{F}_q^r$ donc $s(x)$ est de longueur r et $s(x+y) = h(x+y) = h(x)+h(y) = s(x)+s(y)$. Ceci prouve le point 1 et le point 2. Comme H est de rang r, le nombre d'éléments de l'image est q^r et cette image est l'ensemble des syndromes d'où le point 3.

Par définition d'un mot de code, $x \in C$ si et seulement si $H^t x = 0$ c'est-à-dire si et seulement si $h(x) = 0 \Leftrightarrow s(x) = 0$. Par suite x et y on le même syndrome si et seulement si

$$s(x) = s(y) \Leftrightarrow s(x) - s(y) = 0 = s(x-y) \Leftrightarrow x - y \in C$$

c'est-à-dire si et seulement si x et y sont dans la même classe d'équivalence introduite dans le paragraphe précédent. En particulier si $x^* = x + e$ on a $s(x^*) = s(x) + s(e) = s(e)$ donc le message et l'erreur ont le même syndrome.

Par définition de la matrice d'une application linéaire, les colonnes de H sont les images des éléments de la base donc la colonne h_i représente le syndrome du message $(0,0,0,1,0,0,0)$ dont le *ime* bit est 1 autrement dit d'un message de poids 1. Il y a n message de ce type. Plus généralment si $h_1, h_2, \ldots h_n$ désignent les colonnes de H, tous le syndrome de $x = a_1 a_2 \ldots a_n$ est donné par

$$s(x) = a_1 h_1 + a_2 h_2 + \cdots + a_n h_n$$

On retrouve le résultat précédent lorsque tous les x_i sauf un sont nuls et cela prouve immédiatement le dernier point de notre proposition.

On remplace le tableau standard par la liste des 2^r syndrome avec les messages de plus faible poids dont ils sont les syndromes. Pour établir cette liste on commence par 0 dont le syndrome est bien entendu 0. Puis on calcule les syndromes des messages de poids 1, de poids 2, ... A chaque fois qu'on rencontre un syndrome qui n'est pas dans la liste, on l'ajoute à la liste avec le message qui a permis de le trouver. La liste est terminée lorsque on a trouvé les 2^r syndromes.

Lorsqu'un message arrive à son destinataire, celui-ci calcule son syndrome. S'i n'est pas nul, son message est erroné. Il cherche alors dans sa liste pour trouver le message de plus petit poids ayant le même syndrome. Il corrige alors son message en lui ajoutant (dans le cas binaire) ce message de plus petit poids trouvé.Cette méthode de correction s'appelle (Correction par syndrome)

3.4 Exemple

3.4.1 Les codes BCH

Nous avons montré que les codes de Hamming sont des codes correcteurs d'une erreur. Les codes qui les généralisent qui vont corriger t erreurs sont appelés les codes de Bosz-Chaundri-Hocquenghem (ou B.C.H par abéviation). Nous utilisons alors toute la théorie des corps finis. Nous allons commencer par un exemple. Nous avons vu qu'un code de Hamming de lengueur $n = 2^m - 1$ utilise m bits de contrôle por corriger une erreur. Il est raisonnable de penser que l'utilisation de $2m$ bits de contrôle puisse nous permettre de corriger deux erreurs. Considérons le code de Hamming où $n = 15, m = 4$. Alors la *ime* colonne de la matrice de contrôle est l'expression de i sous forme binaire. Mais nous avons vu aussi que ces colonnes représentent les éléments non nuls du corps fini à 16 éléments $\mathbb{F}_{2^4}$ ce qui se traduit par l'écriture

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \end{pmatrix}$$

Si nous voulons ajouter m bits de contrôle, cela revient à ajouter à la matrice de contrôle H, m autres lignes. Nous noterons la matrice

$$H^{'} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ f(1) & f(2) & f(3) & f(4) & f(5) & f(6) & f(7) & f(8) & f(9) & f(10) & f(11) & f(12) & f(13) & f(14) & f(15) \end{pmatrix}$$

où $f(i)$ désigne la colonne à 4 bits que nous mettons au dessous de la *ime* colonne. Comment allons-nous choisir $f(i),$? Supposons que deux erreurs ont été commises par exemple sur la colonne i et la colonne j. Nous obtenons le syndrôme $s =^t (z_1, z_2)$ qui est égal à la somme des deux colonnes d'indices i et j de $H^{'}$. Il faut donc résoudre le système d'équations

$$i + j = z_1, f(i) + f(j) = z_2$$

Posons $f(i) = i^3$ alors le système devient :

$$i + j = z_1, i^3 + j^3 = z_2$$

On a :

$$(i + j)^3 = i^3 + 3i^2j + 3ij^2 + j^3 = i^3 + j^3 + ij(i + j) = z_2 + z_1ij$$

d'où, puisque $z_1 \neq 0$ (on a supposé deux erreurs donc $i \neq j$)

$$i + j = z_1, ij = z_1^2 + \frac{z_2}{z_1}$$

ce qui signifie i et j sont les solutions du trinôme du second degré

Écrivons la matrice de contrôle sous la forme

$$H = (1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ \alpha^8\ \alpha^9\ \alpha^{10}\ \alpha^{11}\ \alpha^{12}\ \alpha^{13}\ \alpha^{14})$$

alors la matrice $H^{'}$ avec le choix de la fonction $f(i) = i^3$ s'écrit

$$H = \begin{pmatrix} 1\ \alpha\ \alpha^2\ \alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ \alpha^7\ \alpha^8\ \alpha^9\ \alpha^{10}\ \alpha^{11}\ \alpha^{12}\ \alpha^{13}\ \alpha^{14} \\ 1\ \ \alpha^3\ \alpha^6\ \alpha^9\ \alpha^{12}\ 1\ \ \alpha^3\ \alpha^6\ \alpha^9\ \alpha^{12}\ 1\ \ \alpha^3\ \alpha^6\ \alpha^9\ \alpha^{12} \end{pmatrix}$$

Supposons que les deux erreurs ont été commises dans les colonnes 6 et 8. On obtient le syndrome

$$\begin{pmatrix} \alpha^6 \\ \alpha^3 \end{pmatrix} + \begin{pmatrix} \alpha^8 \\ \alpha^9 \end{pmatrix} = \begin{pmatrix} \alpha^6 + \alpha^8 \\ \alpha^3 + \alpha^9 \end{pmatrix}$$

Comme

$$\alpha^6 + \alpha^8 = \alpha^{14}, \alpha^3 + \alpha^9 = \alpha$$

on a donc $z_1 + \alpha^{14}$ et $z_2 = \alpha$ par suite $z_1^2 + \frac{z_2}{z_1} = \alpha^{13} + \alpha^2 = 1 + \alpha^3 = \alpha^{14}$ donc le trinôme est $X^2 + \alpha^{14}X + \alpha^{14}$ qui s'écrit $(X + \alpha^6) + (X\alpha^8)$. On retrouve bien nos erreurs localisées en $i = 6$ et $j = 8$.

Observons que la matrice de contrôle $H^{'}$ exprimée en binaire s'écrit

$$H^{'} = \begin{pmatrix} 1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1 \\ 1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1 \\ 0\,0\,0\,1\,1\,0\,0\,0\,1\,1\,0\,0\,0\,1\,1 \\ 0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1 \\ 0\,1\,1\,1\,1\,0\,1\,1\,1\,1\,0\,1\,1\,1\,1 \end{pmatrix}$$

3.4.2 Les Codes de Reed-Muller

Soit G la matrice génératrice d'un code C ;

$$G = \begin{pmatrix} 1100010 \\ 0110001 \\ 0011101 \\ 0001011 \end{pmatrix}$$

c'est une matrice à 7 colonnes et 4 lignes donc n=7 et k=4. Nous abtenons les mots des codes. En effectuant tout les combainaisons linéaire des 4 lignes i.e en calculant tout les produits $u.G$ lorsque 4 parcourt B^4.

Pour avoir une matrice génératrice standard, nous changeons de base. Effectuons les opèrations suivantes :

1) Nous ajoutons la ligne 4 à la ligne 3, nous abtenons la nouvelle ligne 3 (0010110).

2) Nous ajoutons la ligne 3 à la ligne 2, nous abtenons la nouvelle ligne 2 (0100111)

3) Enfin nous ajoutons la nouvelle ligne 2 à la ligne 1 et nous obtenons la nouvelle ligne 1(1000101)

La matrice génératrice standard est alors

$$G = \begin{pmatrix} 1000101 \\ 0100111 \\ 0010110 \\ 0001011 \end{pmatrix}$$

Comment peut on détrminer la matrice génératrice d'un code ? Comme nous allons le voir dans la suite, certains codes sont définis directement par leur matrice génératrice. (Par exemple les codes Hamming) alors les codes cyclique sont définis à l'aide de leur polynôme générateur. La matrice de contrôle associée est $H = [{}^{-t}p/I_{n-k}]$ donc

$$H = \begin{pmatrix} 1110100 \\ 0111010 \\ 1101001 \end{pmatrix}$$

Soit x^* le message reçu, $x^* = (x_0, x_1, \ldots, x_n)$ le calcule syndrôme à l'aide de la matrice de parité est

$$S(x^*) = (S_0, S_1, \ldots, S_{n-k-1})$$

Si $S(x^*) = 0$ cela signifie que le message reçu est un mot de code. L'étude du décodage est concernée par les syndrôme non nulls. Il s'agit de repérer dans x^* les bits erronés et de les corriger. On trouve que

$$S_i = x_{k+i} + \sum_{j=0}^{k-1} x_j p_{ji}$$

La première terme r_{k+i} est simplement le i^{me} bit de parité reçu par le décodeur. La coefficients de la matrice de parité p et les k bits du message reçu pour les indice allont de 0 à x_{k-1} si la parité reçu et la parité calculleé sont égal la somme de ces parité est alors nulle. [7]

Bibliographie

[1] Par Pierre, Lucas, Louis, de la promotion 2016 de l'ENS UIm, https ://webusers.imj-prg.fr > corps fini.

[2] J.Mellac, CORPS FINIS ET CODES CORRECTEURS D'ERREURS, fevrier 2002,page 6.

[3] Extension de corps généralités, https ://webuser.imj-prg.fr

[4] David Harrari, Algèbre 1-NOTION DE THÉORIE DES CORPS.

[5] Khalifa ZIZI, Groups Anneaux Corps, Office des publications Universitaires :01-2016,page 447-489.

[6] MELAKHESSOU.A, Théorie Algèbrique Des Codes Convolutionnels Cycliques, MEMOIRE :MAGISTER, Université ELHADJ LAKHDAR BATNA, 14.12.2011

Résume

Le but de cette mémoire est : L'étude et la construction de code correcteur d'erreur. Cette tâche feut appel à la théorie des corps fini et certains résultats d'algebre linéaire pour quoi le trail est partagé en trois chapitre

Chapitre 1 : est consacré a l'études des corps finis, les anneaux des polynôme sur un corps fini, les corps fini de décomposition de polynôme irreductible .

Dans le chapitre 2 : ou défini la notion de code linéaire, matrice génératrice, matrice de contrôle, code de Hamming. et ou applique quelques resultats d'algèbre linéaire.

Dans le chapitre 3 : On aborde celle du décodage par tableau standard et de décodage par la méthode syndrome. et donne quelques exemples : code de Hamming, code B.C.H, code de reed-muller.