UNIVERSITE MOHAMED BOUDIAF DE M'SILA

Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Mathématiques**:**

Option :Algèbre et Mathématiques Discrète

Par

DAMMA Saida & LIA Amel

Sujet

Sur le décodage d'un code cyclique

Devant le jury :

Mr D.Mihoubi	Prof. Univ de M'sila	Président
Mr L.Heboub	Prof. Univ de M'sila	Encadreur
Mr N.Ghadbane	Prof. Univ de M'sila	Examinateur

Promotion : 2018 / 2019

Remerciements

Je tiens en premier lieu à exprimer mes plus vifs remerciements à ***Mr. HEBOUB Lakhdar*** *pour l'intéressant de sujet qu'il m'a proposé. Je lui suis également reconnaissant pour la confiance qu'il ma accordée. Il m'est impossible de lui exprimer toute ma gratitude en seulement quelques lignes.*

Je remercie aussi le ***Mr. MIHOUBI DOUADI*** *d'avoir accepté de présider le jury aussi que* ***Mr. GHADBANE NACER*** *d'être membre.*

Je ne saurais oublier de remercier ma famille et mes amis, en particulier mes parents et la famille ***LIA & DAMMA & FEIDJEL*** *pour leur soutient tout au long de mes études.*

A.LIA & S. DAMMA

Table des matières

Notation

$\mathbb{F}_q$: Un corps fini de cardinal q.
$car\,(\mathbb{F}_q)$: Caractéristique d'un corps fini.
$C[n,k]$: Code de longeur n et dimension k.
$d_H(x;y)$: Distance de Hamming entre x et y.
$d(x,y)$: la distance minimale de x et y.
$w(x)$: Poids de Hamming d'un mot x.
$< x,y >$: Le produit scalaire de x et y.
$\left(C^{\perp}\right)$: Le dual de code C.
I_k : Matrice identique de taille $k \times k$.
$d_{\min}$: La distance minimale.
$(f(x))$: idéal engendré par$f(x)$.
$\deg(g(x))$: le degré de polynôme g
$\mathbb{F}_q[x]$: anneau des polynômes à coeffcients dans $\mathbb{F}_q$.
$\mathbb{F}_q[x]/(x^n-1)$: L'annaux quotient.
$Im(\Phi)$: image de Φ.
$ker(\Phi)$: le noyau d'une application Φ.
$\overline{x}$: La classe de x modulo une relation d'équivalence.

Introduction

Les codes correcteurs d'erreurs sont utilisés pour corriger des erreurs quand les messages sont transmis par le biais d'un canal de communication comportant des parasites.

Le transfert de l'information n'est pas parfait, c'est pourquoi il est nécessaire de détecter, et dans certains cas de pouvoir même corriger les erreurs contenues dans le message reçu.

L'enjeu de la détection et de la correction d'erreurs est, donc essentiellement, dans la recherche d'algorithmes de décodage efficaces.

Les codes cycliques, parmi les codes correcteurs, correspondent à ce besoin .

L'objet de ce mémoire est l'étude du problème de décodage des codes cycliques en utilisant les propriétés structurelles des codes cycliques.

Déroulement de la mémoire

Le premier chapitre est un chapitre d'introduction où nous présentons les notions et les propriétés fondamentales nécessaires pour la réalisation de ce travail tels que : anneaux de polynômes, corps finis et espaces vectoriels. Les notions citées dans ce chapitre représentent l'outil mathématique utilisé pour l'étude des codes correcteurs d'erreurs.

Le deuxième chapitre regroupe les définitions et les propriétés fondamentales des codes correcteurs d'erreurs.

Le troisième chapitre est consacré à l'étude de décodage des codes cycliques, nous étudions les définitions et les propriétés des codes cycliques, puis on va présenter la méthode de Meggitt.

.

Chapitre 1

Corps finis

Dans ce chapitre nous rappellons les définitions, les résultats fondamentaux et les notions de base que nous utiliserons dans ce travail, par la suite : groupe, anneau, espace vectoriel, corps et corps fini.

1.1 Groupe

Définition 1.1

Soit G un ensemble non vide muni d' une loi interne " $\cdot$ ", $(G, \cdot)$ est dit groupe si les trois conditions sont vérifiées :

1- la loi "$\cdot$" est associative i.e : $\forall x, y$ et $z \in G$:

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

2- la loi "$\cdot$" a un élément neutre noté e. i.e :

$$\exists e \in G, \forall x \in G x \cdot e = e \cdot x = x.$$

3- Tout éléments de G a un élément symetrique :

$$\forall x \in G, \exists x\prime \in G \; tel \; que \; x \cdot x\prime = x\prime \cdot x = e.$$

Remarque 1.1 Si l'opération "$\cdot$" est commutatif alors le groupe est dit commutatif (abélien).

Exemple 1.1

$(\mathbb{Z}, +)$ est un groupe commutatif.

1.2 Anneau

Définition 1.2

On appelle anneau un ensemble A muni de deux loi de composition interne : l'addition "+"et la multiplication "$\cdot$" tel que :

1. $(A, +)$ est groupe abélien.
2. la multiplication "$\cdot$" est associative et distributive par rapport à l'addition, de plus l'opération "." admet un élément neutre.

i) Si la multiplication est commutatife, c'est-à-dire : $\forall x, y \in A : x.y = y.x$ alors on dit que l'anneau A est commutatife.

ii) Si l'opération "$\cdot$" admet un élément neutre noté 1 ou bien 1_A alors l'anneau A est dit anneau unitaire.

Exemple 1.2

$(\mathbb{Z}, +, \cdot)$ est anneau commutatif unitaire.

Définition 1.3

Soit A un anneau, on dit que A possède des diviseurs de zéro s'il existe $a, b \in A$, $a \neq 0$ et $b \neq 0$ tels que $a \cdot b = 0$. Dans ce cas a est appelé un diviseur de zéro à gauche et b est appelé un diviseur de zéro à droite.

Un anneau A est dit intègre s'il est distinct de $\{0\}$ et s'il ne possède pas de diviseurs de zéro, c'est-a-dire :

$$\forall a, b \in A, \text{si } a.b = 0 \text{ alors } a = 0 \text{ ou } b = 0.$$

Définition 1.4 Soit I un sous ensemble non vide de A, on dit que I est idéal de A si :

1. I est un sous-groupe de $(A, +)$.
2. $\forall a \in I, \forall b \in A, ab \in I$.

L'idéal I est dit principal s'il existe un élément $a \in A$ qui engendre I, c'est-à-dire :

$$I = (a) = \{ar : r \in A\}$$

L'idéal I est dit maximal s'il n'est pas contenu dans un autre idéal J différent de l'anneau A.

Proposition 1.1

Soit I un idéal de l'anneau A, comme I est un sous-groupe de groupe commutatif $(A, +)$, alors I est un sous-groupe normal, et par conséquent on peut former le groupe quotient A/I des classes d'équivalences modulo I. les éléments de A/I sont les classes d'équivalence selon I, c'est-à-dire :

$$A/I = \{I + r, r \in A\}$$

L'addition et la multiplication dans A/I est définit par :

1. $(a + I) \oplus (b + I) = (a + b) + I$.
2. $(a + I) \odot (b + I) = ab + I$.

Avec $a, b \in A$.

Ces opérations confèrent à l'ensemple quotient A/I une structure d'anneau dit anneau quotient.

1.2.1 Anneaux principaux

Définition 1.5

Un anneau A est dit principal s'il est intègre et si tout idéal de A est principal.

Exemple 1.3 $(\mathbb{Z}, +, .)$ est un anneau principal.

1.3 Anneaux des polynômes

Définition 1.6 Soit A un corps commutatif, on note par $A[x]$ l'anneau des polynômes à coefficients dans A. Un élément P de $A[x]$ de degré n s'écrit sous la forme :

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

où $a_i \in A$ pour tout $i \in \{0, 1, \ldots, n\}$.

Le degré de $p \in A[x]$, noté $deg(p)$ est le plus grand entier n tel que $a_n \neq 0$.

Remarque 1.2

Le degré du polynôme nul est moins l'infini $(-\infty)$

Définition 1.7

Soient $P, Q \in A[x]$, On dit que P divise Q et on note $P|Q$ s'il existe $R \in A[x]$ tel que :

$$Q = PR$$

Exemple 1.4

Dans $\mathbb{Z}[x]$ $x - 1$ divise $x^2 - 1, \forall x \geqslant 1$.

Définition 1.8

Un polynôme $P \in A[x]$ de degré $\geqslant 1$ est irréductible sur A, s'il ne possède pas de diviseur $Q \in A[x]$ tel que :

$$1 \leqslant deg(Q) \leqslant deg(P) - 1$$

Un polynôme qui n'est pas irréductible est dit réductible.

Division Euclidienne

Soient $f, g \in K[x]$, on dit que f divise g s'il exist $q \in K[x]$ tel que :

$$g(x) = f(x).q(x)$$

Remarque 1.3 $f \in K[x]$ un polynôme et α un scalaire de K. Alors $f(\alpha) = 0 \Longleftrightarrow (x - \alpha)/f(x)$.

- un polynôme $f \in K[x]$ de dégré n. a au plus n racines.

- un polynôme $f(n) = a_n x^n + ... + a_1 x^1 + a_0$ est dit unitaire (ou normalisé) si $a_n = 1$.

Théorème 1.1 ***(théorème de Bézout)***

Soient $f, g \in K[x]$ et p le pgcd de f et g. Alors il existe deux polynôme u et v de $K[x]$ tel que : $p = u.f + v.g$

Théorème 1.2

Soit $\mathbb{F}$ un corps, chaque idéal de l'anneau des polynôme $\mathbb{F}[x]$ est principal.

Preuve.

Soit I un idéal de $\mathbb{F}[x]$, si $I = \{0\}$ alors I est l'idéal principal (0).

Supposons que $I \neq \{0\}$ et $g(x)$ un polynôme non nul de degré minimal dans I, on montre que $I = (g(x))$, il est évident que $(g(x)) \subseteq I$, reste à prouver que $I \subset (g(x))$.

Soit $f(x) \in I$, la division Euclidienne de $f(x)$ par $g(x)$ donne

$$f(x) = g(x)q(x) + r(x)$$

on a $r(x) = 0$ ou $degr(x) \leq degg(x)$ donc $f(x)$ et $g(x)q(x) \in I$ et par conséquent on a aussi

$$r(x) = f(x) - g(x)q(x) \in I$$

on a donc $r(x) = 0$ ou bien $degr(x) \leq degg(x)$.

on ne peut avoir $degr(x) \leq degg(x)$ ceci contredit l'hypothése que $g(x)$ est le polynôme minimal dans I. On doit avoir donc $r(x) = 0$, et par conséquent :

$$f(x) = g(x)q(x) \in (g(x))$$

■

1.4 Espace vectoriel

Définition 1.9

On dit que E est un espace vectoriel sur un corps K si et seulement si, $\forall u, v, w \in E$

1. $(u + v) + w = u + (v + w)$
2. $\exists 0 : u + 0 = 0 + u = u$
3. $\forall u \exists(-u) : u - u = 0$
4. $u + v = v + u$
5. $\forall c \in K, c(u + v) = c.u + c.v$
6. $\forall a, b \in K, (a + b)u = a.u + b.v$
7. $\forall a, b \in K, (a.b)u = a.(b.u)$
8. $1.u = u$

$F \neq \emptyset$ est un sous-espace vectoriel de E si et seulement si :

$$\begin{aligned} x + y &\in F \qquad \forall x, y \in F \\ \lambda x &\in F \qquad \forall \lambda \in K, \forall x \in F \end{aligned}$$

1.5 Corps finis

Définition 1.10

Un corps est un anneau où tout les éléments non nuls sont inversible.

Définition 1.11

Un corps finis d'order q est aussi appelé corps de Galois qu'un note GF(q) ou $\mathbb{F}_q$.

Définition 1.12

Soit K un corps quelconque, qu'on appelle sous-corps premier de K le plus petit sous-corps de K.

Exemple 1.5 Si p est premier $\mathbb{F}q = Z/pZ$ est un corps fini. $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$ ..... sont des corps premiers.

Extension de corps fini

Pour E un corps et F un sous-corps de E. on dit que E est une extension de F.

Exemple 1.6

1. Le corps C est une extension de $\mathbb{R}$.
2. Le corps $\mathbb{Q}(\sqrt{2})$ est une extension de $\mathbb{Q}$ ($\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2}, a, b \in \mathbb{Q}\right\}$

1.5.1 Caractéristique d'un corps fini

Le nombre p est appelé la caractéristique du corps $\mathbb{F}_q$, Il est noté par car($\mathbb{F}_q$)

$$car\left(\mathbb{F}_q\right) = inf\left\{n \in N^*, n.1 = 0\right\}$$

Théorème 1.3

Soit $\mathbb{F}_q$ un corps fini. Alors :

1) La caractéristique de $\mathbb{F}_q$ est un nombre premier p.

2) $\mathbb{F}_q$ est un espace vectoriel de dimension finie sur $\mathbb{F}_p$ et on a : q=p^n.

Définition 1.13

Un groupe G est dit cyclique s'il existe $g \in G$ telque $G =< g >$. L'élément g est un générateur du groupe G :

$$G = \left\{1, g, ..., g^{n-1}, \text{ avec } g^n = 1_G.\right\}$$

Théorème 1.4

Soit $\mathbb{F}_q$ un corps fini de cardinal q. Le groupe multiplicatif $(\mathbb{F}_q^*, \times)$ est cyclique d'ordre $q - 1$.

Théorème 1.5

Soit $\mathbb{F}_q$ un corps fini de cardinal q.

Pour tout $x \in \mathbb{F}_q^*$ on a : $x^{q-1} = 1$, et pour tout $x \in \mathbb{F}_q$ on a : $x^q = x$.

Théorème 1.6 *(théorème de Wedderburne)*

Tout corps fini est commutatif.

Proposition 1.2

Soit F_q, $q = p^m$ un corps fini de caractéristique p, alors :
$\forall x, y \in \mathbb{F}_q : (x+y)^{p^i} = x^{p^i} + y^{p^i}, \quad i \in N^*$.

1.5.2 Factorisation de $\mathbf{x}^n - 1$

Polynôme minimal

Définition 1.14

Soit $\alpha \in \mathbb{F}_{q^m}$, le polynôme minimal de α sur $\mathbb{F}_q$ est le polynôme unitaire de plus bas degré $f(x) \in \mathbb{F}_q[x]$ vérifiant $f(\alpha) = 0$. Nous le notons $M_\alpha(x)$.

Proposition 1.3

Soit $\alpha \in \mathbb{F}_{q^m}$, soit d un entier positif non nul. Le degré du polynôme minimal $M_\alpha(x)$ sur $\mathbb{F}_q$ est égal à d si et seulement si d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$. Rappelons que l'ordre de α (dans le groupe multiplicatif $\mathbb{F}^*_{q^m}$) est le plus petit entier positif non nul l tel que $\alpha^l = 1$.

Lemme 1.1

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α, i.e $\alpha^l = 1$. Soit d un entier positif non nul. Alors d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$ si et seulement si $d = ord_l(q)$.
Preuve.

Notons $r = ord_l(q)$. D'aprés la définition de l'ordre de q modulo l, nous avons $l \mid q^r - 1$. Mais $\alpha^l = 1$, donc $\alpha^{q^r-1} = 1$ et $\alpha^{q^d} = \alpha$. Et r est le plus petit entier positif non nul avec cette propriété,

compte tenu de la même définition. Donc r est égal à d si et seulement si d est le plus petit entier positif non nul tel que $\alpha^{q^d} = \alpha$. ■

Corollaire 1.1 *Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α Alors :*

$$\deg M_\alpha(x) = ord_l(q).$$

tel que $l \in \{1, 2, ..., q^m - 1\}$

Preuve.

C'est une conséquence directe de la proposition et du lemme précédent. ■

Proposition 1.4

Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α Alors

$$M_\alpha(x) = \prod_{i=0}^{ord_l(q)-1} \left(x - \alpha^{q^i}\right) = \prod_{i=0}^{d-1} \left(x - \alpha^{q^i}\right),$$

c'est-à-dire $\left\{\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots, \alpha^{q^{ord_l(q)-1}}\right\}$ est l'ensemble des racines de $M_\alpha(x)$.

Remarque 1.4

La proposition et le corollaire précédent nous montrent que

$$\alpha^{q^{ord_l(q)}} = \alpha.$$

Proposition 1.5

Soit $\alpha \in \mathbb{F}_{q^m}$. Toutes les racines de $M_\alpha(x)$ sont de même ordre.

Conjugaison

La conjugaison dans $\mathbb{F}_{q^m}$ est la relation R définie par

$$\alpha R \beta \quad \text{si} \quad M_\alpha(x) = M_\beta(x) \ .$$

Proposition 1.6

La conjugaison dans $\mathbb{F}_{q^m}$ est une relation d'equivalence.

Définition 1.15 Les conjugués d'un élément α de $\mathbb{F}_{q^m}$ sont les éléments de la classe d'equivalence de α pour la conjugaison dans $\mathbb{F}_{q^m}$.

Proposition 1.7 *Soit $\alpha \in \mathbb{F}_{q^m}$. Soit l l'ordre de α. Les conjugués de α sont*

$$\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots, \alpha^{q^{ord_l(q)-1}}.$$

Ils sont distincts deux à deux.

Preuve.

C'est une conséquence directe de la définition précédente et de la proposition dans polynôme minimal. ■

Remarque 1.5

En résumé, tous les éléments de $\mathbb{F}_{q^m}$ sont divisés en classes d'équivalence pour la conjugaison. Une classe déquivalence est composée de toutes les racines d'un polynôme minimal sur $\mathbb{F}_q$ Donc :

1. il y a autant des classes d'équivalence que de polynômes minimaux différents des éléments de il y a autant des classes de $\mathbb{F}_{q^m}$.
2. le cardinal de toute classe est égal au degré du polynôme minimal correspondant.

Racines de l'unité

Rappelons que $(n, q) = 1$. Soit m un entier positif non nul tel que $n \mid q^m - 1$.

Définition 1.16

On appelle racine n-ièmes de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ dont l'ordre divise n, on appelle racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ d'ordre n. En particulier si $n = q^m - 1$, une racine primitive n-ièmes de l'unité sur $\mathbb{F}_q$ est un élément primitif de $\mathbb{F}_{q^m}$.

Proposition 1.8 *Les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe du groupe multiplicatif $\mathbb{F}_{q^m}^*$.*

En effet, si β et γ sont deux racines n-ièmes de l'unité sur $\mathbb{F}_q$, $(\beta\gamma)^n = \beta^n\gamma^n = 1$ et donc $\beta\gamma$ est aussi une racine n-ièmes de l'unité sur $\mathbb{F}_q$. D'ailleurs, $\left(\beta^{-1}\right)^n = (\beta^n)^{-1} = 1$. Donc les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous groupe de $\mathbb{F}_{q^m}^*$. Comme $\mathbb{F}_{q^m}^*$ est cyclique, ce sous groupe est aussi cyclique.

Soit μ l'entier tel que $\mu \cdot n = q^m - 1$. Soit α un élément primitif de $\mathbb{F}_{q^m}$. Alors β est une racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$, car l'ordre de α^u est égal à $\frac{q^m-1}{(q^m-1,u)} = \frac{q^m-1}{u} = n$. Donc β est un générateur de ce sous-groupe qui est dordre n. Ce sous-groupe est composé de toutes les racines de $x^n - 1$, i.e. la décomposition de $x^n - 1$ sur $\mathbb{F}_{q^m}$ est

$$x^n - 1 = \prod_{i=0}^{n-1} \left(x - \beta^i\right).$$

Soit γ une racine n-ièmes de l'unité sur $\mathbb{F}_q$. Ses conjugués dans $\mathbb{F}_{q^m}$ sont les puissances de γ, donc ils sont aussi des racines n-ièmes de l'unité sur $\mathbb{F}_q$. La conjugaison dans $\mathbb{F}_{q^m}$ définit donc une relation d'équivalence dans l'ensemble des racines n-ièmes de l'unité sur $\mathbb{F}_q$. On peut alors dire les mêmes choses comme dans la remarque précédent chaque classe d'équivalence est composée de toutes les racines d'un polynôme minimal, et

1- il y a autant des classes d'équivalence que de polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$.

2- le cardinal de toute classe est égal au degré du polynôme minimal correspondant.

Nous obtenons aussi que

$$x^n - 1 = \prod_{\gamma} M_\gamma(x),$$

où parcourt un ensemble de représentants des classes d'équivalence, et compte tenu de la proposition dans la partie polynôme minimal, que le polynôme minimal de $\gamma = \beta^j$, $j \in \mathbb{Z}_n$, est égal à

$$M_\gamma(x) = \prod_{i=0}^{ord_l(q)-1} \left(x - \gamma^{q^i}\right) = \prod_{i=0}^{ord_l(q)-1} \left(x - \beta^{jq^i}\right)$$

où l est l'ordre de γ, $l = \frac{n}{(n,j)}$.

Cas général Prenons maintenant le cas général ou n et q ne sont pas forcément premiers entre eux. Soit $n = rp^s$, ou r est premier avec p et $s \geq 0$ (p^s est la plus grande puissance de p qui divise n). Alors

$$x^n - 1 = x^{rp^s} - 1 = (x^r - 1)^{p^s},$$

car nous travaillons sur le corps $\mathbb{F}_q$ de caractéristique p.

Puisque r est premier avec p, nous pouvons décomposer $x^r - 1$ comme ci-dessus, et en déduire la décomposition de $x^n - 1$. Plus précisément, si β est une racine r-ième primitive de l'unité sur $\mathbb{F}_q$, alors

$$x^r - 1 = \prod_{i=0}^{r-1} \left(x - \beta^i\right)$$

et donc

$$x^n - 1 = (x^r - 1)^{p^s} = \left(\prod_{i=0}^{r-1} \left(x - \beta^i\right)\right)^{p^s} = \prod_{i=0}^{r-1} \left(x - \beta^i\right)^{p^s}$$

De même,

$$x^n - 1 = (x^r - 1)^{p^s} = \left(\prod_{\gamma} M_\gamma(x)\right)^{p^s} = \prod_{\gamma} M_\gamma(x)^{p^s}.$$

où parcourt un ensemble de représentants des classes d'équivalence par conjugaison des racines r-ièmes de l'unité sur $\mathbb{F}_q$.

Classes cyclotomiques

Soit $(n, q) = 1$.

Soit β une racine n-ièmes primitive de l'unité sur $\mathbb{F}_q$. La relation d'équivalence sur les racines n-ièmes de l'unité sur $\mathbb{F}_q$, induit une relation d'équivalence dans l'ensemble $\mathbb{Z}_n$ comme suit : $i, j \in \mathbb{Z}_n$ sont dans la même classe d'équivalence si et seulement si β^i et β^j sont dans la même classe. À la classe de $\gamma = \beta^j$, i.e. la classe $\left\{\gamma, \gamma^q, \gamma^{q^2}, \gamma^{q^3}, \ldots, \gamma^{q^{r-1}}\right\} = \left\{\beta^j, \beta^{jq}, \beta^{jq^2}, \beta^{jq^3}, \ldots, \beta^{jq^{r-1}}\right\}$, correspond la classe des exposants $\{j, qj, q^2j, \ldots, q^{r-1}j\}\, mod\ n$, où r est le nombre de conjugués distincts de β^j. Nous savons que r est le plus petit entier positif non nul tel que $(\beta^j)^{q^r} = \beta^j$, autrement dit, tel que $jq^r \equiv j\ mod\ n$.

Définition 1.17

Pour tout entier j, $j \in \mathbb{Z}n$, nous définissons la classe cyclotomique de j modulo n

sur $\mathbb{F}_q$ comme l'ensemble

$$Cl(j) = \left\{j, qj, q^2j, \ldots, q^{r-1}j\right\} mod\ n,$$

où r est le plus petit entier positif non nul tel que $jq^r \equiv j\ mod\ n$.

Nous pouvons donc réécrire les résultats. Nous avons que

$$r = \deg M_{\beta^j}(x) \equiv ord_l(q),$$

où l est l'ordre de β^j, nous obtenons que le polynôme minimal de $\gamma = \beta^j$, $j \in \mathbb{Z}_n$, est

$$M_\gamma(x) = \prod_{i \in Cl(j)} \left(x - \beta^i\right).$$

Le nombre de classes cyclotomiques modulo n sur $\mathbb{F}_q$ est égal au nombre de polynômes minimaux différents des racines n-ièmes de l'unité sur $\mathbb{F}_q$. La formule nous donne

$$x^n - 1 = \prod_j M_{\beta^j}(x),$$

où j parcourt un ensemble de représentants des classes cyclotomiques modulo n sur $\mathbb{F}_q$. Donc le nombre de classes cyclotomiques modulo n sur $\mathbb{F}_q$ est égal au nombre de diviseurs irréductibles de $x^n - 1$ sur $\mathbb{F}_q$.

Décomposition de $x^n - 1$ sur $\mathbb{F}_q$

Définition 1.18

Soit $(n, a) = 1$. Le plus petit entier positif non nul r tel que $a^r \equiv 1 \bmod n$ est appelé l'ordre de a modulo n et noté $ord_n(a)$.

Si $a \geq 1$, l'order $ord_n(a)$ de a modulo n est l'order de a dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

algorithme de décomposition

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 $L = \mathbb{F}_{q^m}$.

2. Détermination des différentes classes cyclotomiques $(i, iq, iq^2, ..., iq^j, ...)$. 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 L).

Exemple 1.7

Considérons $x^7 - 1$ sur $\mathbb{F}_2$ on a $n = 7$, $q = 2$ et $m = 3$ car $7 = 2^3 - 1$

Pour les classes cyclotomique modulo 7 on a :

$$\begin{aligned} C_0 &= \left\{0, 2^j\right\} = \{0\} \\ C_1 &= \left\{1, 2^j\right\} = \{1, 2, 4\} = C_2 \\ C_3 &= \left\{3, 2^j\right\} = \{3, 5, 6\} \end{aligned}$$

Les trois polynôme minimaux sont :

$$\begin{aligned} M_0(x) &= (x-1) \\ M_1(x) &= \prod_{j \in C_1} \left(x - \alpha^j\right) = (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) \\ M_3(x) &= \prod_{j \in C_3} \left(x - \alpha^j\right) = \left(x-\alpha^3\right)\left(x-\alpha^5\right)\left(x-\alpha^6\right) \end{aligned}$$

(α une racine 7-ième primitive de l'unité sur $\mathbb{F}_2$).

Pour déterminierles cofficients binaire de $M_1(x)$ et $M_3(x)$, il faut faire des calculs dans $\mathbb{F}_8$, puis que $8 = 2^3$, nous considéronsun polynôme binaire de degré 3 irréductible sur $\mathbb{F}_2$, par exemple $f(X) = x^3 + x + 1$ si α racine primitive de $f(x)$, alors $f(\alpha) = 0$.

On a donc

$$\alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1, \alpha^7 = 1$$

Alors

$$\begin{aligned} M_1(x) &= (x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right) = x^3 + \left(\alpha + \alpha^2 + \alpha^4\right)x^2 + \left(\alpha^3 + \alpha^5 + \alpha^6\right)x + \alpha^7 \\ &= x^3 + x + 1 \end{aligned}$$

Et la factorisation de $x^7 - 1$ sur $\mathbb{F}_2$

$$x^7 - 1 = (x+1)\left(x^3 + x^2 + 1\right)\left(x^3 + x + 1\right)$$

1.5.3 Construction d'un corps fnis

On va montrer que pour tout nombre premier p et m un entier strictement positive on peut construire un corps de cardinal p^m.

Soit $\mathbb{F}$ un corps alors $\mathbb{F}[x]$ est un anneau principal. c-à-d pour tout idéal I dans $\mathbb{F}_q[x]$ on a $I = (p(x))$ où $p(x)$ est un polynôme non nul de plus petit degré dans I.

Soit $p(x) \in \mathbb{F}_q[x]$, l'idéal engendré par $p(x)$ est

$$(p(x)) = \mathbb{F}_q[x]/(p(x)) = \{p(x)g(x) : g(x) \in \mathbb{F}_q[x]\}$$

et l'anneau quotient $\mathbb{F}[x] = p(x)$ est

$$\mathbb{F}[x] = p(x) = \{f(x) + I : f(x) \in \mathbb{F}[x]\}$$

on note $f(x) + I$ par $\overline{f(x)}$ ainsi $\overline{p(x)} = \overline{0}$ cet anneau est muni des opération :
L'addition : $\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}$
La multiplication : $\overline{f(x).g(x)} = \overline{f(x)} \cdot \overline{g(x)}$

Théorème 1.7

Soit $\mathbb{F}$ un corps et soit $p(x)$ un polynôme irréductible non constant dans $\mathbb{F}[x]$. Alors il existe une extension E de $\mathbb{F}$ et un élément $\alpha \in E$ tel que $p(\alpha) = 0$.

Preuve.

Soit souhaitons trouver une extension E de $\mathbb{F}$ contenant un élément tel

que $p(\alpha) = 0$. L'idéal $p(x)$ engendré par $p(x)$ est un idéal maximal dans $\mathbb{F}_q[x]$, alors $\mathbb{F}[x] = p(x)$ est un corps .

Nous prétendons que $E = \mathbb{F}[x]/p(x)$ est le corps désiré.

Nous montrons tout d'abord que E est une extension de $\mathbb{F}$.

Nous pousons définir un hommorphisme d'anneaux commutatifs par l'application :

$$\begin{aligned} \Psi &: \mathbb{F} \longrightarrow \mathbb{F}[x]/p(x), avec \\ \Psi(\alpha) &= a + (p(x)) pour a\alpha \in F \end{aligned}$$

il est facile de vérifie qu'il s'agit d'un hommorphisme d'anneaux.

on a :

$$\Psi(a) + \Psi(b) = (a + p(x)) + (b + p(x)) = (a + b) + p(x) = \Psi(a + b)$$

et

$$\Psi(a)\Psi(b) = (a + p(x))(b + p(x)) = ab + p(x) = \Psi(ab)$$

L'applicationΨ est injective car :

$\Psi(a) = \Psi(b) \Longrightarrow a + (p(x)) = b + (p(x)) \Longrightarrow a - b$ multiple de $p(x)$ puisque le polynôme $p(x)$ non constant, la seule possibilité et que $a - b = 0$ alors $a = b$

Nous pousons identifie $\mathbb{F}$ avec le sous-corps $\{a + (p(x)) : a \in \mathbb{F}\}$ de E.E une extention de $\mathbb{F}$.

Il nous reste à prouver que $p(x)$ à un zero $\alpha \in E$.

On pose $\alpha = x + (p(x))$ alors dans E.

Si $p(x) = a_0 + a_1x + ... + a_nx^n$ alors

$$\begin{aligned} p(\alpha) &= a_0 + a_1(x + p(x)) + ... + a_n(x + p(x))^n \\ &= a_0 + a_1x + ... + a_nx^n + (p(x)) = 0 + (p(x)) \end{aligned}$$

par conséquent, nous avons trouvé un élément $\alpha \in E = \mathbb{F}[x] = p(x)$ *tel que* $p(\alpha) = 0$.

■

Exemple 1.8

Construire de $\mathbb{F}_9$"corps fini à 9 éléments"

Dans $\mathbb{F}_3$, le polynôme $p(x) = x^2 + x + 2$ est irréductible sur $\mathbb{F}_3[x]$, on détermine les éléments de $\mathbb{F}_{3^2}$ en le regardant comme extension est obtenue par adjonction à $\mathbb{F}_3$ d'une racine de $p(x)$, ainsi $\mathbb{F}_{3^2} = \mathbb{F}_3[x]\diagup(p(x))$, soit α une racine de $p(x)$, alors $\{1, \alpha\}$

est une base de $\mathbb{F}_{3^2}$.

$\mathbb{F}_3[x]/(p(x)) = \{a_0 + a_1\alpha / a_0, a_1 \in \mathbb{F}_3\} = \{0, 1, 2, \alpha, 2\alpha, 1+\alpha, 2+\alpha, 1+2\alpha, 2+2\alpha\}$
(Représentation polynômiale) :

Tout polynôme de corps $\mathbb{F}_3[x]/(p(x))$ peut être modulo $p(x)$ en utilisant le fait que :

$$p(\alpha) = 0.$$

Dans $\mathbb{F}_3$, c-à-d que : $\alpha^2 + \alpha + 1 = 0$ et on aura :

$\mathbb{F}_{3^2} = \mathbb{F}_3[x]/(p(x))$

$= \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$ (Représentation en puissance de α)

Chapitre 2

Le principe de codage

La théorie des codes, qui date du millieu du XX^{e} siècle, permet de transmèttre a travers d'un canal bruit. Donc, cette théorie joue aujourd'hui un rôle fondamental dans les systèmes modernes de transmission et de stokage de l'information numérique.

dans cette partie nous commencerons par énoncer quelque généralités sur la théorie des codes puis nous présenterons les codes linéaires et les méthodes de décodage du codes linéaires.

2.1 Code

Définition 2.1

Un code sur A de longueur n est un sous-ensemble C de A^n, l'ensemble A est appelé l'alphabet, n la longeur du code C, un code $C \subset A^n$ est de cardinalité M si $M = |C|$ et les éléments de C sont appelés les mots du code.

où l'alphabet est un ensemble quelconque finie et non vide.

Exemple 2.1

1. le code $C = \{(011010), (111011), (111111), (110000), (011100)\}$ est un code de longueur 6 sur l'alphabet $A = \{0, 1\}$.
2. $C = \{aabb, mmmm, accc, zzkk\}$ est un code de logueur 4 et de cardinal 4 sur l'alphabet de la language française.

Distance De Hamming

Définition 2.2 Soient $x = (x_1, x_2, ..., x_n)$ et $y = (y_1, y_2, ..., y_n) \in \mathbb{F}_q^n$, La distance de hamming de x et y est le nombre $d_H(x, y)$ défini par :

$$d_H(x, y) = \left|\left\{i = \overline{1, n} : x_i \neq y_i\right\}\right|$$

On remarque que la distance de hamming sur $\mathbb{F}_q^n$ est une vrie distance au sens numérique de terme. Rappelons briévement les propriétés d'un distance $d_H(x, y)$:

1. $d_H(x, y) = 0 \iff x = y$;
2. $d_H(x, y) = d_H(y, x) \geq 0$;
3. $d_H(x, y) \leq d_H(x, z) + d_H(z, y)\ \forall x, y, z \in \mathbb{F}_q^n$.

Exemple 2.2

Dans $\mathbb{F}_3^2$ nous avons $d_H(010, 100) = 2$, $d_H(010, 000) = 1$.

La distance minimal d'un code

La distance minimale du code C est la distance minimum entre deux mots distincts de code défini par :

$$d = Min\left\{d_H(x, y) : x, y \in C, x \neq y\right\}$$

Définition 2.3 Un code $[n, M, d]$ sur $\mathbb{F}_q$ est un code de longueur n, de taille M et de distance minimal d.

$[n, M, d]$ sont les paramètre de C.

Le poids de Hamming

Définition 2.4 Le poids de Hamming d'un mot $x = \{x_1, x_2, ..., x_n\}$, noté $w(x)$, est le nombre d'indice i telle que $x_i \neq 0$.

$$w_H(x) = |\{i/x_i \neq 0\}| = d(x, 0)$$

Exemple 2.3

par exemple, dans $\mathbb{F}_2^3$, nous avons $w(101) = 2$ et $w(001) = 1$.

Définition 2.5

Le poids minimal d'un code C est définit par :

$$w(x) = \min \{w_H(x) : x \in C, x \neq 0\}$$

2.2 Code linéaire

Définition 2.6

Un code linéaire de paramètres $[n, M, d]$ est un sous-espace vectoriel de dimension k de $\mathbb{F}_q^n$, de distance minimale d. On a alors une application de codage linéaire

$$\Phi_C : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$$

Remarque 2.1

1. La dimension d'un code linéaire est sa dimension comme sous-espace vectoriel.
2. Si C est un code linéaire de dimension k sur $\mathbb{F}_q$, alors : $M = q^k$.
3. Si $\{c_1, c_2, ..., c_k\}$ une base de C, le code C est l'ensemble :

$$\left\{ \sum_{i=1}^{K} a_i c_i, a_i \in \mathbb{F}_q \right\}$$

4. Si x et y sont deux mots de code, alors $x + y$, $x - y$, et $(\forall a \in \mathbb{F}_q, ax \in C)$ sont des mots de codes.

Exemple 2.4

1. le code $C = \{000, 001, 110, 101, 100, 011, 010, 111\}$ est un code linéaire de longueur 3 sur $\mathbb{F}_2$ de dimension 3.
2. $C = \{(000000), (001110), (010101), (011011), (100011), (101101), (110110), (111000)\}$ est code linéaire de dimension 3 de longueur 6.
3. $C = \{(00000), (11100), (00111), (11011)\}$ est un code linéaire de longeur 5.

Proposition 2.1

Si le code C est linéare on a :

$$d = \min_{x \in C, x \neq 0} w(x)$$

Preuve.

En effet

$$d = \min_{x,y \in C, x \neq y} d(x,y) = \min_{x,y \in C, x \neq y} d(x-y,0) = \min_{c \in C, c \neq 0} w(c)$$

■

Matrice génératrice d'un code linéaire

Comme l'application Φ étant linéaire, alors le code C peut être définit par une matrice génératrice G de type $k \times n$ sur $\mathbb{F}_q$, dont les lignes forment une base de C sur $\mathbb{F}_q$, on obtient donc l'application linéaire qu'on note Φ_G au lieu de Φ_C définit par :

$$\begin{array}{rcl} \Phi_G & : & \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n \\ x & \mapsto & xG \end{array}$$

Par conséquent, on a la proposition suivante.

Proposition 2.2

Soit C un code linéaire de paramètres $[n,k]$ sur $\mathbb{F}_q$, si G est une matrice génératrice de C alors :

$$C = \operatorname{Im} \Phi_G = \left\{ xG, x \in \mathbb{F}_q^k \right\}$$

où $\operatorname{Im} \Phi_G$ est l'image de $\mathbb{F}_q^n$ par l'application Φ_G.

Exemple 2.5 Soit C un code linéaire sur $\mathbb{F}_q$ de matrice génératrice :

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

on a $q = 2, k = 2$

$C = \{mG, m \in \mathbb{F}_2^2\} = \{(m_1, m_1 + m_2, m_1 + m_2) : m_1, m_2 \in \mathbb{F}_2\}$

$C = \{(000), (011), (100), (111)\}$.

La matrice de contôle

On peut obtenir le code C, comme étant le noyau d'une application linéaire dont les lignes de la matrice H associée forment une base de l'espace nul de la matrice génératrice G.

Rappelons dans ce contexte que si A est une matrice $m \times n$ sur le corps $\mathbb{F}$. L'espace nul de A est l'ensemble de $v \in \mathbb{F}^n$ tel que :

$$Av^t = 0$$

L'espace nul de A est un sous-espace de $\mathbb{F}^n$ et sa dimension est appelée nullité de A, on a :

$$rangA + nullitéA = n$$

Le rang de la matrice G étant égal à k, on a :

$$nullitéG = n - k = rangH$$

on obtient donc l'application linéaire

$$\begin{array}{rcl} \Phi_H & : & \mathbb{F}_q^n \to \mathbb{F}_q^{n-k} \\ x & \mapsto & H^t x \end{array}$$

alors le code C est l'ensemble :

$$C = \ker \Phi_H = \left\{ x \in \mathbb{F}_q^n : \Phi_H(x) = H^t x = 0 \right\}$$

Remarque 2.2 La matrice H permet de savoir si un élément quelconque $x \in \mathbb{F}_q^n$ est un mot de code où non, c'est pour quoi est appelée la matrice de contrôle du code C.

Le code dual

Définition 2.7 Soient $x, y \in \mathbb{F}_q^n$,le produit scalaire de x et y donné par :

$$\langle x, y \rangle = x_1 y_1 + x_2 y_2 + ... + x_n y_n$$

Si $\langle x, y \rangle = 0$ alors on dit que x est orthogonal à y.

Définition 2.8

On a C est un code linéaire de paramètres $[n, k, d]$ le code dual de C est l'ensemble $C^{\perp}$ défnit par :

$$C^{\perp} = \left\{ y \in \mathbb{F}_q^n : \langle x, y \rangle = 0, \forall x \in C \right\}$$

Remarque 2.3

1. Si C est un code linéaire de paramètres $[n, k]$, le code dual de C est un code linéaire de paramètres$[n, n-k]$.
2. La matrice de contrôle d'un code C est une matrice génératrice de son dual $C^{\perp}$.

Code systématique

Une matrice génératrice G est dit sous forme systématique si ellle s'écrit :

$$G = (I_K \mid A)$$

avec I_k est la matrice unité a k lignes et k colonnes, et A une matrice de taille $k \times (n-k)$.

dans ce cas la matrice de contrôle de C est de la forme :

$$H = \left(-{}^tA \mid I_{n-k} \right)$$

de plus, si $H = (B \mid I_{n-k})$, alors $G = (I_k \mid -{}^tB)$.

Exemple 2.6 Soit C un $[4, 2]$ code linéaire sur $\mathbb{F}_3$ de matrice génératrice G alors :

$$G = \begin{pmatrix} 1 & 0 & .. & 2 & 2 \\ 0 & 1 & .. & 2 & 1 \end{pmatrix} \Rightarrow H = \begin{pmatrix} -2 & -2 & .. & 1 & 0 \\ -2 & -1 & .. & 0 & 1 \end{pmatrix} \Rightarrow H = \begin{pmatrix} 1 & 1 & .. & 1 & 0 \\ 1 & 2 & .. & 0 & 1 \end{pmatrix}$$

2.2.1 Décodage d'un code linéaire

Dans ce paragraphe nous présentons les définitions et les principes de détection et correction d'erreurs, puis on va présenter deux méthodes de décodage du codes linéaires : décodage par tableau standard et décodage par syndrôme, avec des exemples.

Définition 2.9

Soit $x \in \mathbb{F}_q^n$ un mot de code envoyé et $y \in \mathbb{F}_q^n$ le message reçu. On appelle vecteur erreur

$$e = x - y = (e_1, e_2, ..., e_n) \in \mathbb{F}_q^n$$

et le nombre d'erreurs $N = d(x, y)$.

Proposition 2.3

Soit C un $[n, M, d]$ code sur $\mathbb{F}_q$, le code C détecte au plus $d-1$ erreurs et corrige au plus $\left[\frac{d-1}{2}\right]$ erreurs.

Décodage par tableau standard

Soit C un code linéaire de dimension k sur $\mathbb{F}_q$ i.e C un s.e.v de $\mathbb{F}_q^n$, on peut former l'espace quotient $\mathbb{F}_q^n/C = \mathbb{F}_q^n/R$, dont la relation d'équivalence R est définie par :

$$\forall x, y \in \mathbb{F}_q^n : xRy \iff x - y \in C$$

$\mathbb{F}_q^n/C$ est l'ensemble des classes d'équivalence de la forme :

$$\overline{a} = a + C = \{a + x : x \in C\}$$

et $a \in \mathbb{F}_q^n$.

Chaque classe contient $|\overline{a}| = |C| = q^k$ éléments. On obtient la partition

$$\mathbb{F}_q^n = C \cup \left(a^{(1)} + C\right) \cup ... \cup \left(a^{(t)} + C\right)$$

avec t=$\frac{\left|\mathbb{F}_q^n\right|}{|C|} - 1 = \frac{q^n}{q^k} - 1 = q^{n-k} - 1$.

Soit x un mot de code transmit et $y \in \mathbb{F}_q^n$ l'élément reçu, y doit être dans l'une des classes $a^{(i)} + C$, le vecteur erreur $e = y - x \in a^i + C - x = a^{(i)} + C$ (car C est un code linéaire $C - x = C$) et par conséquent l'erreur commise e est dans la classe de $y = a^{(i)} + C$. L'erreur minimale est obtenue en prenant l'élément de poids minimal qu'on appelle chef de classe on décode y par le mot de code $x = y - \alpha$.On fait remarque que si α est le chef de classe de $a^{(i)} + C$, on $a + C = a^{(i)} + C$. Cette règle de décodage conduit à construire le tableau standard (table de SLEPAIN).

Soient $\alpha_1, \alpha_2, ..., \alpha_n$ les chefs de classe.

$$\left.\begin{array}{llll} c_1 = 0 & c_2 & ... & c_q^k \\ \alpha_1 + c_1 & \alpha_1 + c_2 & ... & \alpha_1 + c_q^k \\ \alpha_2 + c_1 & \alpha_2 + c_2 & ... & \alpha_2 + c_q^k \\ ... & ... & ... & ... \\ \alpha_t + c_1 & \alpha_t + c_2 & ... & \alpha_t + c_q^k \end{array}\right\} \begin{array}{l} \text{la classe des mots de code} \\ \\ \text{autres classes} \\ \\ \\ \end{array}$$

Si y est vecteur reçu on cherche y dans le tableau, disant $y = \alpha_i + c_i$, on décode y par $x = y - \alpha_i = \alpha_i + c_i - \alpha_i = c_i$, c-à-d le mot de code de la même colonne.

Exemple 2.7

On cherche à transmettre des messages α de longueur 2 sur l'alphabet $\{0, 1\}$ au moyen du $(4, 2)$-code linéaire définit par la matrice génératrice G suivante :

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

On observe que G n'est pas sous forme standard ,on transforme alors G en ajoutant à la ligne 1 la ligne 2 et on obtient la matrice génératrice $G\prime$ d'un code équivalent qui est sous forme standard :

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

l'ensemble des messages non codés correspond aux différets couples possibles sur $\{0, 1\}$ qui sont :

$$A = \{(00), (01), (10), (11)\}$$

On peut alors énumérer les différents mots du code en effectuant le produit à gauche des éléments $\alpha \in A$ par la matrice $G\prime$:

$$\begin{array}{ccc} \textit{mots de } A & \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} & \textit{poids} \\ (00) & (0000) & \\ & & 2 \\ (01) & (0101) & \\ & & 3 \\ (10) & (1011) & \\ & & 3 \\ (11) & (1110) & \\ & \textit{mots du code} & \end{array}$$

Le code C est donc composé du mots :

$$C = \{0000, 0101, 1011, 1110\}$$

Le poids minimal des mots de C donne la distance minimale du code qui est 2. Le code C est donc un $(4, 2, 2)$ −code linéaire.

Si on veut transmettre le message (10), il suffit d'effectuer le produit

$$(10)\,.\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \Big(\underbrace{01}_{\text{symboles d'information}} \qquad\qquad \underbrace{11}_{\text{bits de redondance}}\Big)$$

Afin de corriger une erreur, le décodeur costruit le tableau standard suivant :

0000	0101	1011	1110	← mots de C
1000	1101	0011	0110	
0100	0001	$\underline{1111}$	1010	
0010	0111	1001	1100	
$\underset{\text{chef de classe}}{\uparrow}$				

obtenu à l'aide des classes latérales :

$$\begin{aligned} 0000 + C &= C \text{ lui-même} \\ 1000 + C &= \{1000, 1101, 0011, 0110\} \\ 0100 + C &= \{0100, 0001, 1111, 1010\} \\ 0010 + C &= \{0010, 0111, 1001, 1100\} \end{aligned}$$

Observons que la classe latérale $0001 + C$ est identique à la classe latérale $0100 + C$ puisque $0001 \in 0100 + C$.

Si on suppose avoir reçu le message 1111, on vérifie facilement que ce n'est pas un mot du code. Pour trouver de quel mot du code il provient, on cherche sa position dans le tableau standard et on lit le mot du code qui est dans la même colonne sur la première ligne. Le vecteur d'erreur se lit sur la même ligne dans la première colonne. Ainsi, le message transmis était 1011avec 0100 comme vecteur d'erreur.

Le syndrôme

Le décodage par syndrôme est une technique générale de décodage des codes linéaires ayant un coût meilleur que celui de la recherche exhaustive dans plusieur cas.

Soit C un code linéaire de paramètres $[n, k, d]$, et H une matrice de cotrôle de C. On définit l'application

$$\begin{aligned} S &: \mathbb{F}_q^n \to \mathbb{F}_q^{n-k} \\ x &\mapsto S(x) = H^t x \end{aligned}$$

avec $S(x)$ est le syndrôme du vecteur x.

Définition 2.10

On appelle un code t-correcteur un code qui corrige juqu-à t-erreurs.

Lemme 2.1

Soit C un code t-correcteur , et soit $x \in \mathbb{F}_q^n$, on a :

1)$S(x) = 0 \Leftrightarrow x \in C$.

2) si $y = x + e; x \in C$; alors $S(y) = S(e)$.

3)Soit $x_1, x_2 \in \mathbb{F}_q^n$, si $S(x_1) \leq t$ et $S(x_2) \leq t$, alors $S(x_1) = S(x_2) \Rightarrow x1 = x2$.

Preuve.

1)Trivial, (par difinition de S).

2)Si $y = x + e$ avec $x \in C$, alors $S(y) = S(x + e) = S(x) + S(e)$.

car C est linéaire,et comme $x \in C : S(x) = 0$, donc $S(y) = S(e)$.

3)Si $w(x_1) \leq t$ et $w(x_2) \leq t$,alors $w(x_1 - x_2) \leq 2t \leq d$.

de plus $S(x_1) = S(x_2) \Rightarrow S(x_1 - x_2) = 0 \Rightarrow x_1 - x_2 \in C$, donc $x_1 x_2 \in C$,

$w(x_{1-}x_2) \prec t \Rightarrow x_1 - x_2 = 0$. ■

Décodage par syndrôme

Soit $C[n, k]$ un code linéaire t-correcteur de matrice de contrôle H. Voici une méthode pour décoder tout mot reçu $y \in \mathbb{F}_q^n$ prouvu que y soit détecter d'au plus t erreurs :

$y = c + e_y$ avec $c \in C$ et $w(e_y) \leq t$.

on considère toute les erreurs éventuelles, céest-à-dire tous les $e \in \mathbb{F}_q^n$ tel que $w(e) \leq t$. Pour chaque $e \in \mathbb{F}_q^n$ tel que $w(e) \leq t$, on calcul $S(e)$.

D'aprés l'assertion 3 du lemme : si $e_1 \neq e_2$ alors $S(e_1) \neq S(e_2)$. On fait une table contenant ces informations. Soit $y = c + e_y \in \mathbb{F}_q^n$ un mot reçu, on calcule$s = S(y)$, on sait que $s = S(e_y)$.

[i] si s figure dans la table, associé à e_0, en décode y par $y - e_0$.

[ii] si non, on peut dire que y est affecté de plus de t erreurs et on ne peut pas décodé.

Cette méthode de décodage est efficace mais couteûse .Remarquons d'autre part que même dans le cas [i] on fora une erreur de décodage si,en fait, y est affecter de plus de t erreurs.

Le décodage des codes liniaires par syndrôme s'effectue en suivre les étapes :

i) Calcul du syndrôme du mot réçu y.

ii) Détermination de la classe latériale associée.

iii) Recherche dans cette classe du mot errur e (de poids au plus e).

iiii) Calcul de $x = y - e$.

Exemple 2.8 On prend la matrice génératrice $G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ du code linéaire de paramètres $[4, 2]$, et on calcule la matrice de cotrôle $H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$

On calcule ensuite les syndrômes $S(e)$ des chefs de classe e par $H^t e$:

$$S\,(0000) = 00, S(1000) = 11, S(0100) = 01, S(0010) = 10$$

on construit la table :

$syndrômes\ z$	$chefs\ de\ classe\ f(z)$
00	0000
11	1000
01	0100
10	0010

Si on suppose avoir reçu le message $y = 1111$, on calcule le syndrômes

$$S(y) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} . \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = (01)$$

On en déduit que le mot du code est $x = y - f(01) = 1111 - 0100 = 1011$ et que le vecteur erreur était (0100) .

Chapitre 3

Décodage d'un code cyclique

3.1 Introduction

Dans ce chapitre nous allons présenter les codes cycliques qui présentent la famille du codes la plus importante. D'un point de vue pratique ce sont les codes les plus utilisés, car leur mise en oeuvre est facile, et ils admettent souvent de bons algorithmes de décodage, avec des théorèmes, notions et des exemples sur ce type des codes. Ensuite, nous présentons une méthode de décodage des codes cyclique.

3.2 Codes cycliques

Définition 3.1

Soient $\mathbb{F}_q$ un corps finis, et $n \in \mathbb{N}^*$.

C un code linéaire sur $\mathbb{F}_q^n$, on dit que C est cyclique si vérifier :

$$(c_0, c_1, ..., c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, c_2, ..., c_{n-2}) \in C$$

Exemple 3.1

1. Le code $C = \{000, 101, 011, 110\}$ est un code cyclique.
2. Le code $C = \{0000, 1001, 0110, 1111\}$ n'est pas cyclique. Il est cependant équivalent à un code cyclique (il faut échanger les troisième et quatrème coordonnées).

Représentation polynomial

On appelle représentation polynomial l'application θ définie par :

$$\theta : \mathbb{F}_q^n \to \mathbb{F}_q[x] \diagup (x^n - 1)$$

$$(c_0, c_1, ..., c_{n-1}) \mapsto c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

La représentation de $c = c_0 c_1 ... c_{n-1}$ est le polynôme $c(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$.

La représentation polynomial d'un code C est l'ensemble des représentations polynomials de ces mots .En effectuer un décalage sur un mot reviet à multiplier par x sa représentation polynomial modulo $x^n - 1$.Donc C est cyclique si et seulement si pour tout mot c de code C ,$xC(x)$ calculé modulo $x^n - 1$ est la représentation polynomial d'un mot de C, en pratique, on confond les mots de code et leur représentation polynomial.

Exemple 3.2

Le code $C = \{000, 110, 011, 101\}$ correspand aux polynôme $0, 1 + x, x + x^2, 1 + x^2$ pris modulo $x^3 - 1$.

3.3 Polynôme générateur

Définition 3.2

Le polynôme générateur $g(x)$ d'un code cyclique C est un polynôme non nul unitaire de plus bas degré de C.

Exemple 3.3

Soit C un $[7, 3]$ code cyclique, donc $g(x) = 1 + x^2 + x^3 + x^4$ est un polynôme générateur de C.

Théorème 3.1

La dimension d'un code cyclique de longueur n et de polynôme générateur $g(x)$ est :

$$k = n - \deg g(x)$$

Théorème 3.2

Le polynôme générateur est unique.

Preuve.

Supposons que g_1, g_2 soient deux polynôme générateurs, alors $g_1 - g_2$ est un polynôme générateur (le code est linéaire) de degré stictement inferieur au degré de g_1 contradiction. ■

Lemme 3.1

Le polynôme générateur du code cyclique C divise $x^n - 1$.

Preuve.

Ce résultat permettra de construire les codes cycliques à partir des diviseurs de $x^n - 1$. Pour la preuve, on calcule la dicision euclidienne de $x^n - 1$ par $g(x)$ dans $\mathbb{F}_q[x]$, et on conclut en passant modulo $x^n - 1$, ce qui donne :

$$0 = q(x)g(x) + r(x) \in C$$

ainsi

$$r(x) = -q(x)g(x) \in C$$

donc

$$r(x) = 0$$

■

Théorème 3.3

Soit C un code cyclique de longueur n, et soit $g(x)$ son polynôme générateur, alors :le code C est l'ideal pricipal $\langle g(x) \rangle$ de l'anneau $R_n = \mathbb{F}_q[x] \diagup (x^n - 1)$

Exemple 3.4

Sur $\mathbb{F}_2[x]$ on a

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

Dans $\mathbb{F}_2[x] \diagup (x^3 - 1)$, soit C_1, C_2 les codes générés respecyivement par les polynôme $g_1(x) = 1 + x$, $g_2(x) = 1 + x + x^2$

alors on a :

$$C_1 = \{0, 1+x, x+x^2, 1+x^2\} = \{000, 110, 011, 101\}$$

$$C_2 = \{0, 1+x+x^2\} = \{000, 111\}$$

Notons que le code C_1 est aussi généré par le polynôme $1+x^2$ .Toute fois $g_1(x)$ est l'unique polynôme unitaire, de degré minimal, générateurs de C.

Représentation matricielle

C un code cyclique de longueur n sur $\mathbb{F}_q$, de polynome générateur

$$g(x) = g_0 + g_1 x + ... + g_{n-k} x^{n-k}$$

une matrice génératrice de C est une matrice de type $k \times n$ donné par :

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 \\ \cdots & ... & ... & \cdots & ... & \cdots & ... & ... \\ 0 & 0 & \cdots & \cdots & g_0 & g_1 & \cdots & g_{n-k} \end{pmatrix}$$

Exemple 3.5

Considérons le code cyclique C de $\mathbb{F}_2^7$ engendré par le polynôme générateur $g(x) = 1 + x^2 + x^3$. donc une matrice génératrice de ce code est donné par :

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

Chaque ligne de G peut être obtenue par un shift de la présidente.

Définition 3.3 Soit C un $[n, k, d]$ un code cyclique de polynôme générateur $g(x)$, le polynôme :

$$h(x) = \frac{(x^n - 1)}{g(x)}$$

est dit le polynôme de contrôle.

Maintenant l'expression de la matrice de contrôle est :

$$\begin{pmatrix} h_k & h_{k-1} & ... & h_0 & 0 & ... & 0 \\ 0 & h_k & h_{k-1} & ... & h_0 & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... \\ 0 & ... & 0 & h_k & h_{k-1} & ... & h_0 \end{pmatrix}$$

3.4 Construction d'un code cyclique

Pour construire un code cyclique de longueur n, il est utile de connaître la décomposition de $x^n - 1$ en polynômes irréductibles sur le corps de base $\mathbb{F}$

$$x^n - 1 = \prod_i f_i(x).$$

En l"absence d'un logiciel (maple, magma,...), on peut déterminer les classes cyclotomiques modulo n. Le nombre de classes donne le nombre de facteurs irréductibles. La donnée d'un polynôme irréductible divisseur de $x^n - 1$ permet alors de connaître tous les autres facteurs. Le polynôme générateur du code est un produit d'un certain nombre de facteurs trouvés.

Exemple 3.6

Combien peut-on construire de codes cycliques $[31, 21]$ sur $\mathbb{F}_2$.

Il suffit de déterminer les classes cyclotomiques modulo 31.Il exicte 7 classes cyclotomiques, chacune contenant 5 éléments

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8, 16\} \\ C_3 &= \{3, 6, 12, 24, 17\} \\ C_5 &= \{5, 10, 20, 9, 18\} \\ C_7 &= \{7, 14, 28, 25, 19\} \\ C_{11} &= \{11, 22, 13, 26, 21\} \\ C_{23} &= \{23, 15, 30, 29, 27\} \end{aligned}$$

Il existe 6 facteurs de degré 5 et un facteur de degré 1 : $(x-1)$. Le polynôme générateur d'un code $[31, 21]$ doit être de degré 10. Il y a $\binom{6}{2} = 15$ possibilités. Pour pouvoir factoriser effectivement $x^{31}-1$ il faut connaître un polynôme irréductible de degré 5(en effet $31 = 2^5 - 1$). Il existe des tables qui donnent des polynômes irréductibles ou primitifs de degré donné sur $\mathbb{F}_2$.

3.5 Décodage des codes cycliques

3.5.1 Introduction

Soit un code cyclique $C(n, k, d)$ sur $\mathbb{F}_q$ et soit $c(x) \in C$ le mots envoyé et $y(x)$ et reçu, $e(x) = y(x) - c(x)$ et le polynôme erreur. nous définirons le poids d'un polynôme comme le nombre de coefficients non nul.

Rappelons aussi que si t est la capacité de correction de C et si $z(x) \in \mathbb{F}_q[x]/(x^n-1)$ on dira que $\ll z(x)$ est le mot reçu dont l'erreur est $e(x) \gg$. Si $w(e(x)) \leq t$ et s'il existe $c(x) \in C$ tel que :

$$z(x) = c(x) + e(x)$$

(c'est à dire, $z(x)$ provient d'un mot de C entaché d'un nombre d'erreur au plus égale à t).

Il nous reste maintenant à voir ce que l'on entend par le syndrôme d'un polynôme.

3.5.2 Syndrôme d'un polynôme

Définition 3.4

Soit C un code cyclique de polynôme générateur $g(x)$.On appelle syndrôme polynomial d'un mot $z(x) \in \mathbb{F}_q[x]/(x^n-1)$, le reste de la division de $z(x)$ par $g(x)$ dans $\mathbb{F}_q[x]$. on le note $S(z(x))$.

Il est clair que $z(x) \in C \implies S(z(x)) = 0$

et que $S(z(x)) = S(z'(x)) \iff z(x) - z'(x) \in C$.

Ainsi cette définition de syndrôme est équivalente à celle, présentée pour les codes linéaires.

Propriété Soit un mot $z(x) \in \mathbb{F}_q[x]/(x^n-1)$, alors $z(x) \in C$ si et seulement si $g(x)$ divise $z(x)$ dans $\mathbb{F}_q[x]$.

Le décodage des codes cycliques s'effectue généralement en 3 étapes :

· Calcul du syndrôme.

· Assosiation du syndrôme à l'erreur correspondante grâce à une table.

· Ajout de l'erreur au mot reçu.

Exemple 3.7

Soit C un code cyclique $(7,4,3)$ sur $\mathbb{F}_2$ de polynôme générateur $g(x) = x^3+x+1$.

Le code C corrige seulement une erreur, donc on à le tableau de syndrômes suivant :

Réprésentants de classes	syndrôme
1	1
x	x
x^2	x^2
x^3	$x+1$
x^4	x^2+x
x^5	x^2+x+1
x^6	x^2+1

Supposons alors que ayant transmis $c(x) = x+x^2+x^3+x^6$, nous ayons reçu $y(x) = x+x^3+x^6$, calculons son syndrôme or

$x+x^3+x^6 = (x^3+x)(x^3+x+1)+x^2$.

Donc $S(y(x)) = x^2$.

Le représentant de la classe x^2 étant x^2, on décode $y(x)$ de la façon suivante

$$c(x) = y(x) - x^2 = x+x^2+x^3+x^6.$$

Qui est bien le mot qui avait été envoyé.

Donc nous présentons la méthode de décodage de Meggitt.

Décodage de Meggitt

Supposons $C(n,k,d)$ un code cyclique sur $\mathbb{F}_2$ de polynôme générateur $g(x)$, C corrigera $t = \left[\frac{d-1}{2}\right]$ erreurs. Supposons que $c(x) \in C$ est envoyé et $y(x) = c(x) + e(x)$ est reçu, où $e(x)$ est le vecteur erreur avec $w\left(e\left(x\right)\right) \leq t$.

Donc on présente une technique pour le décodage des codes cycliques nommé le décodage de meggitt.

La méthode de décodage de Meggitt s'applique aux codes cycliques binaires, mais elle peut se généraliser au cas non binaires, l'idée de base consiste en l'utilisation de la cyclicité du code pour restreindre la table des syndrôme et permettre des calculs récursifs. La méthode s'appuie sur le résultat suivant :

Proposition 3.1

Soit $e\left(x\right)$ le mot erreur du mot reçu $y(x)$. Alors, pour tout entier, $0 \leq j \leq n-1$.

1. le mot $x^j y(x)$ est un mot reçu l'erreur est $x^j e(x)$.
2. $S(x^j e(x)) = S(x^j y(x))$.

(Tout les produits sont calculés dans $\mathbb{F}_2\left[x\right]/\left(x^n-1\right)$).

Proposition 3.2

Avec les notations de la proposition précédente soit $S_i(x)$ la suite de polynômes de $\mathbb{F}_2\left[x\right]/\left(x^n-1\right)$ définie par :

$$S_0\left(x\right) = S\left(y\left(x\right)\right) ... S_{i+1}\left(x\right) = S\left(xS_i\left(x\right)\right).$$

Alors pour tout entier $0 \leq j \leq n-1$.

$$S_j(x) = S(x^j y(x)).$$

Exemple 3.8

Soit C un code cyclique $(7,4)$ sur $\mathbb{F}_2$ de polynôme générateur

$$g(x) = x^3 + x^2 + 1.$$

Soit le mot reçu $y(x) = x^4 + x^3 + x^2 + 1$ le syndrôme du mot reçu est le reste de la division euclidienne de $y(x)$ par $g(x)$.Donc

$$\begin{aligned} S_0(x) &= S(y(x)) = 1 + x + x^2. \\ S_1(x) &= S(xy(x)) = 1 + x. \\ S_2(x) &= S\left(x^2 y(x)\right) = x + x^2 \end{aligned}$$

Principe du décodage

Le décodeur de Meggitt effectue un décodage symbole par symbole. On corrige d'abord une composante erronée du mot reçu au moyen de la méthode décrite ci-dessous, puis on applique de nouveau la méthode au nouveau mot reçu ainsi obtenu.

Algorithme de décodage de Meggitt

Soit T la table des syndrômes des erreurs dont la composante d'indice $n-1$ est erronée. Soit $c(x)$ le mot envoyé, $y(x)$ le mot reçu, et $e(x)$ le moterreur avec $w(e(x) \leq t$.

La suite $S_i(x)$ est définie comme dans la proposition (3.2).

· Calcule de $S(y(x))$.

· Si $S(y(x)) = 0$ alors $c(x) = y(x)$ et l'algorithme se termine.

· Si non.

· Rechercher le plus petit entier j tel que $S_j(x)$ se trouve dans la table T

· Corriger la composante d'indice $n-1-j$ de $y(x)$, soit $y'(x)$ le nouveau mot obtenu.

· Repartir au début de l'algorithme avec $y'(x)$.

Exemple 3.9

Soit C le code Hamming $(7, 4, 3)$ sur $\mathbb{F}_2$, et soit $g(x) = x^3 + x + 1$ le polynôme générateur, le code Hamming binaire est un code 1-Correcteur, la table T des syndrômes des erreurs dont la composante d'indice 6 est égale à 1 se reduit au tableau suivante :

erreur	x^6
syndrôme	$x^2 + 1$

-Soit $y(x) = x^6 + x^4 + x + 1$ le mot reçu, le syndrôme est le reste de la division de $y(x)$ par $g(x)$, c'est-à-dire

$$x^6 + x^4 + x + 1 = (x^2 + x + 1)(x^3 + 1) + 0.$$

Donc $S(y(x)) = 0$, alors le mot envoyé est $y(x)$.

-Soit $y(x) = x^6 + x^3 + x$, le mot reçu , le syndrôme est le reste de la division de $y(x)$ par $g(x)$:

$$x^6 + x^3 + x = \left(x^3 + x + 1\right)\left(x^3 + 1\right) + x^2.$$

Donc $S(y) = x^2$, or $S(y(x))$ ne figure pas dans la table T, et $j = 4$ est le plus petit entier tel que $S_j(x) \in T$, il y a donc une erreur en position 2 avec l'hypotèse que la capacité de correction égale à 1 n'est pas dépassé, léerreur est $e(x) = x^2$ et le mot envoyé est :Soit

$$c(x) = x^6 + x^3 + x^2 + x.$$

Exemple 3.10

Soit C $[35, 12, 18]$ le code cyclique sur $\mathbf{F}_q$ de polynôme générateur

$g(x) = x^{23} + x^{22} + 2x^{21} + 2x^{20} + x^{19} + x^{18} + x^{17} + 2x^{15} + x^{13} + x^{12} + x^{11} + 2x^{10} + x^9 + 2x^7 + x^5 + x^4 + x^2 + 2.$

La table$T$ des syndrômes des erreurs dont la composante d'indice 34 est erronée se réduit au tableau suivant :

erreur x^{34}

Syndrôme $x^{22} + x^{21} + 2x^{20} + 2x^{19} + x^{18} + x^{17} + x^{16} + 2x^{14} + x^{12} + x^{11} + x^{10} + 2x^9 + x^8 + 2x$

$2x^{34}$
$2x^{22} + 2x^{21} + x^{20} + x^{19} + 2x^{18} + 2x^{17} + 2x^{16} + x^{14} + 2x^{12} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^6 + 2x^4$

Soit $y(x) = x^{33} + x^{23} + x^{22} + 2x^{21} + 2x^{20} + x^{19} + x^{18} + x^{17} + 2x^{15} + x^{13} + x^{12} + x^{11} + 2x^{10} + x^9 + 2x^7 + x^5 + x^4 + x^2 + 2$, le mot reçu le syndrômes de $y(x)$ est

$S(x) = x^{21} + x^{20} + 2x^{19} + 2x^{18} + x^{17} + x^{16} + x^{15} + 2x^{13} + x^{11} + x^{10} + x^9 + 2x^8 + x^7 + 2x^5 + x^3 + x^2 + 1$

On recherche le petit entier j tel que $S_j(x) \in T$.

j	$S_j(x)$
0	$x^{21}+x^{20}+2x^{19}+2x^{18}+x^{17}+x^{16}+x^{15}+2x^{13}+x^{11}+x^{10}+x^9+2x^8+x^7+2x^5+x^3+x$
1	$x^{22}+x^{21}+2x^{20}+2x^{19}+x^{18}+x^{17}+x^{16}+2x^{14}+x^{12}+x^{11}+x^{10}+2x^9+x^8+2x^6+x^4+$

on trouve $j = 1$ le petit entier j tel que $S_j(x) \in T$,donc on a une erreur en position $35-1-1=33$ avec l'hypothèse que la capacité de correction égal a 8 n'est pas dépassée $e(x) = x^{33}$

et le mot envoyé est

$y\prime(x) = y(x) - e(x) = y(x) - x^{33} = x^{23} + x^{22} + 2x^{21} + 2x^{20} + x^{19} + x^{18} + x^{17} + 2x^{15} + x^{13} + x^{12} + x^{11} + 2x^{10} + x^9 + 2x^7 + x^5 + x^4 + x^2 + 2$

car $S(x) = 0$.

Conclusion

Nous avons présenté dans ce travail une étude sur les techniques de décodage des codes cycliques qui est basée sur les propriétés structurelles des codes cycliques. On a présenté la méthode de décodage de Meggitt. Cette méthode se base sur le fait que le nombre d'erreur ne dépasse pas la capacité de correction.

Bibliographie

[1] C. **Mihoubi**, Classification des Codes linéaires tertiaires optimaux [n,n/2], These de Doctorat, Université Hadj Lakhdar Batna, 2012.

[2] **S. Ameur**, Etude sur les bornes des codes correcteurs d'erreurs, Thèse de Magister en Mathématiques,Université de M^{ed} Boudiaf m'sila, 2000.

[3] **H. Lakhdar,** Etude de Techniques de décodage des codes linéaires, Thèse de Magister, Université de M'sila 2009/2010.

[4] **O.papini et J.wolfman**, Algèbre discrète et codes correcteurs, Springer Vergal 1995.

[5] **S.Gintaras**, Calcul du groupe d'automorphismes des codes. Détermination de l'équivalence des codes, Université de limoges, 1999.

[6] **M.Demazure**, Cours d'algèbre. Primalité, divisibilité, codes, Nouvelle bibliothéque mathématique, Cassini, 1997.

[7] M.**Bruno**, Codage, cryptologie et applications, presses polytechniques et universitaires romaindes 2004.

[8] **K. Sofiane**, Codes cycliques Iso-duaux de Rendement $1/2$ sur $GF(2)$, mémoire de Master, Université de M^{ed} Boudiaf m'sila, 2014.

[9] corps finis, cour master S_1 (cours sur internet).

[10] **A.Regouid,M.Bahache,** sur les codes cycliques minimaux,mémoire de Master, Université de M^{ed} Boudiaf m'sila, 2017.

[11] **Thomas W. Judson, Stephen F. Austin,** Abstract Algebra : Theory and Applications, Free Software Foundation, Boston, August 27, 2010.

خلاصة

يندرج هدا العمل في إطار فك الشفرات الدورية و الذي يهدف لإيجاد الرسالة الأصلية المرسلة عبر قناة اتصال انطلاقا من الرسالة المستقبلة. في البداية نقدم المفاهيم الأساسية لنظرية الشفرات المصححة لأخطاء ثم نتطرق إلى طرق فك الشفرات الدورية مستعملين.

- طريقة Meggitt.

الكلمات المفتاحية : الحقول المنتهية، الشفرات الدورية.

Résumé

Ce travail se situe dans le cadre de décodage des codes cycliques qui consiste à déterminer le message original envoyé via un canal de transmission, à partir du message reçu. Tout d'abord nous présentons les concepts fondamentaux de la théorie des codes correcteurs d'erreurs ensuite, nous abordons les méthodes de décodage des codes cycliques, en utilisant:

-la méthode de Meggitt.

Mots clés: corps finis, codes cycliques.

Abstract

This work is included in the frame of the theory of the decoding cyclic codes that consist in determining the original message sent through a canal of transmission using the received message. First we present the basic concepts of the theory of error correcting codes then we discuss the methods of decoding cyclic codes, using :

-The method of Meggitt.

Key words: Finite Fields, cyclic codes.