REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématiques Discrète

Thème

Sur les idempotents primitifs de codes cycliques irréductibles

Présentée par :
Kouidri Cherifa
Hamza Khadidja

Devant le jury composé de :

MIHOUBI Douadi	Prof,	Université de M'sila	**Président**.
GHADBANE Nacer	M.C.A,	Université de M'sila	**Examinateur.**
HABOUB Lakhdar	M.A.A,	Université de M'sila	**Encadreur.**

Année universitaire 2019/2020

REMERCIEMENT

Tout d'abord, Nous tenons à remercier ALLAH tout-puissant et Miséricordieux qui nous a donné la force et la patience d'accomplir ce travail. En second lieu, nous tenons à exprimer notre reconnaissance à notre encadreur Mr L.Heboub Nous le remercions de nous avoir encadrés, orientés aidés et conseillés. Tout notre respect et nos remerciements vont vers les membres du jury qui vont pleinement consacrer leur temps et leur attention afin d'évaluer notre travail qui espérons le sera à la hauteur de leur attente. Enfin, nos remerciements les plus sincères sont adressés à toutes personne qui participé de près ou de loin à la réalisation de ce modeste mémoire.

Table des matières

Introduction

La théorie des codes correcteur d'erreurs a pour but la création de codes capables de détecter et éventuellement de corriger des erreurs survenus lors de la transmission d'un message, parmi ces codes, Les codes cycliques qui sont importants car il ne nécessitent que très d'informations pour être très facilement implémentés grâce au registre à décalages . Beaucoup de codes importants en pratique sont des codes cycliques. Ce travail est subdivisé en trois chapitres :

Le premier chapitre est consacré à une introduction où nous présentons les notions les propriétés fondamentales nécessaires pour la réalisation de ce travail tels que : anneaux, anneaux principaux, anneaux de polynômes, corps fini et construction d'un corps finis.

Le deuxième chapitre est consacré à l'étude des codes, codes linéaires, et plus précisement les codes cycliques et les codes cycliques minimaux.

Enfin, dans le troisième chapitre, on va étudier les idempotents primitifs d'un code cyclique où nous explorons autre méthode pour d'écrire les codes cycliques.

Chapitre 1

Les corps finis

Dans ce chapitre, on rappelle les notions de base dont on aura besoin par la suite tels que : corps, corps fini, extension d'un corps, Construction d'un corps fini, polynôme minimal et factorisation de $x^n - 1$ sur un corps fini.

1.1 Rappel sur les anneaux

Définition 1.1.1 *On appelle anneau un ensemble non vide A muni de deux lois 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.*

• *Si la multiplication est commutatif, c'est-à-dire : $\forall x; y \in A : x \cdot y = y \cdot x$ alors on dit que l'anneau A est commutatif.*
• *Si l'opération "." admet un élément neutre noté 1 ou bien 1_A alors l'anneau A est dit anneau unitaire.*

Exemple 1.1.1 *$(\mathbb{Z}, +, .)$ est anneau commutatif unitaire.*

Définition 1.1.2 *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 1.1.3 *Soit I un sous ensemble non vide de A, on dit que I est un **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 :*

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

• *Un idéal de A est dit propre s'il est différent de A.*

Définition 1.1.4 *Un idéal I de A est premier si*

$$I \neq A \text{ et } \forall x, y \in A, x.y \in I \Longrightarrow x \in I \text{ ou } y \in I.$$

Définition 1.1.5 *L'idéal I est maximale dans A si $I \neq A$ et si $I \subset J$ alors, $J = I$ ou $J = A$.*

Exemple 1.1.2 *Les idéaux maximaux dans $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$ avec p premier.*

Définition 1.1.6 *Soit A un anneau commutatif unitaire. Un anneau A est dit **principal** s'il est intègre et si tout idéal de A est principal.*

Exemple 1.1.3 *$(\mathbb{Z}, +, .)$ est un anneau principal.*

Définition 1.1.7 *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 :*

$$p(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

où $a_i \in A$ pour tout $i \in \{0, 1, ..., n\}$, $a_n \neq 0$. Le degré de $p \in A[x]$, noté $\deg(p)$.

Remarque 1.1.1 *Le degré du polynôme nul est moins l'infini* $(-\infty)$.

anneau quotient

Supposons que I est un idéal dans l'anneau A. Pour chaque $a \in A$, on peut former l'ensemble

$$a + I = \{a + i \mid i \in I\}$$

qui est appelle une classe de I. On peut montrer que $a + I = b + I$ si et seulement si $a - b \in I$, et que deux classes $a + I$ et $b + I$ sont disjoints. Les classes (distincts) peut être transformée en un anneau lui-même avec addition et multiplication définie par :

$$(a + I) \oplus (b + I) = (a + b) + I.$$

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

L'anneau de tous les classes de I est appelé **anneau quotient** et est noté par A/I.

Exemple 1.1.4 *Soit* $A = \mathbb{K}[x]$ *un anneau de polynômes,* $f(x) \in \mathbb{K}[x]$ *de degré* n, $I = (f(x)) = \{h(x)f(x) \mid h(x) \in A\}$. *Alors* $A/I = \mathbb{K}/(f(x))$ *anneau quotient. Soit* $g(x) \in A$. *On distinct deux cas :*

1. *Si* $\deg(g) < n = \deg(f)$ *donc* $\overline{g(x)} = g(x) + I \in A/I$.

2. *Si* $\deg(g) \geq n$ *Par la division euclidienne de* g *par* f *dans* $\mathbb{K}[x]$, *il existe* $q(x)$,$r(x) \in \mathbb{K}[x]$ *tel que :*$g(x) = q(x).f(x) + r(x)$ *on a :*

$$\overline{g(x)} = \overline{q(x).f(x)} + \overline{r(x)} = \overline{0} + \overline{r(x)} = \overline{r(x)}.$$

En résument :

$$\begin{aligned} \mathbb{K}[x]/(f(x)) &= \{g(x) + I / \deg g < \deg f\} \\ &= \{a_0 + a_1 x + ... + a_{n-1}x^{n-1} + I / a_i \in \mathbb{K}\} \end{aligned}$$

1.2 Corps fini

Définition 1.2.1 *Un corps est un anneau commutatif dans lequel tout élément non nul est inversible.*

• *Si* $(\mathbb{K}, +, \cdot)$ *est un corps, un sous corps de* $\mathbb{K}$ *est un sous anneau* $\mathbb{K}_1$ *de* $\mathbb{K}$ *tel que pour tout élément non nul* x *de* $\mathbb{K}_1$ *, on a* $x^{-1} \in \mathbb{K}_1$ *;* $(\mathbb{K}_1, +, .)$ *est alors un corps.*

Exemple 1.2.1

1. $\mathbb{Q}$ *corps des nombres rationnels,*
2. $\mathbb{R}$ *corps des nombres réels,*
3. $\mathbb{C}$ *corps des nombres complexes.*
4. $\mathbb{Z}$ *ensemble des entiers relatifes n'est pas un corps, mais c'est un anneau.*

Définition 1.2.2 *Un corps finis* $\mathbb{F}$ *est un corps ayant un nombre fini d'éléments. Le nombre d'éléments dans* $\mathbb{F}$ *est appelé* ***l'ordre*** *de* $\mathbb{F}$*.*

Nous désignerons un corps avec q éléments par $\mathbb{F}_q$, une autre notation courante est **GF(q)** et lire, le corps de **Galois** avec q éléments.

Caractéristiques d'un corps fini

Définition 1.2.3 *Soit* K *un corps d'élément neutre* 1_K*. Le noyau du morphisme défini par :*

$$\mathbb{Z} \to K$$

$$n \to \overbrace{1_K + 1_K + ... + 1_K}^{n\ fois}$$

est, en tant qu'idéal de l'anneau principal $\mathbb{Z}$*, de la forme* $p\mathbb{Z}$ *pour* $p \geq 0$ *appelé la caractéristique de* K *et on note par* $Car(K)$*.*

Exemple 1.2.2 $\mathbb{Q}$ *est de caractéristique 0.*

Lemme 1.2.1 *La caractéristique* $\boldsymbol{p}$ *d'un corps est soit nulle soit un nombre premier.*

Théorème 1.2.1 *Si p est un nombre premier, alors les entiers* $\bmod p, GF(p)$, *constituent un corps. Chaque corps finis F contient un sous-corps qui est $GF(p)$, pour certains p premier et $p \cdot \alpha = 0$ pour chaque α dans F.*

Théorème 1.2.2 *Théorème de Wedderburn.*
Tout corps fini est commutatif.

Lemme 1.2.2 *Si K est un corps fini de caractéristique p, alors*

$$(a+b)^{p^i} = a^{p^i} + b^{p^i}$$

pour tout a,b $\in K$ et $i \in \mathbb{N}^*$.

Démonstration 1.2.1 *On raisonne par récurrence sur i. Si $i = 1$, la formule du binôme de Newton s'écrit*

$$(a+b)^p = \sum_{m=0}^{p} C_p^m a^m b^{p-m}$$

et l'on vérifie que tous les coefficients C_p^m sont divisibles par p dès que $0 < m < p$. En effet, de $p-(p-1)....(p-m-1) = m!C_p^m$ on déduit que p divise $m!C_p^m$. Comme p est premier, il est premier avec tout nombre qu'il ne divise pas, donc en particulier avec chacun des facteurs du produit m!. p est donc premier avec m! , et comme il divise le produit $m!C_p^m$ il divisera C_p^m d'après le Théorème de ***Gauss****. On aura donc $(a+b)^p = a^p + b^p$ Enfin si la propriété est vraie jusqu'au rang i,*

$$(a+b)^{p^{i+1}} = [(a+b)^{p^i}]^p = [a^{p^i} + b^{p^i}]^p = a^{p^{i+1}} + b^{p^{i+1}}.$$

Structure d'un corps fini

Définition 1.2.4 *Un polynôme $p \in \mathbb{F}[x]$ ($\mathbb{F}$ corp) est dit* ***irréductible*** *s'il ne peut être factorisé en deux polynômes de degré au moins égal à 1. Autrement dit, s'il n'existe pas deux polynômes q et q' dans $\mathbb{F}[x]$ de degré au moins égal à 1 tel que $p = q \cdot q'$.*

Théorème 1.2.3 *K est un anneau. Soit $\mathbb{F}$ un corps et $f(x) \in \mathbb{F}[x]$ un polynôme irréductible, L'anneau quotient $K = \mathbb{F}[x]/(f(x))$ est un corps .De plus K contient un sous corps isomorphe à $\mathbb{F}$.*

Preuve 1.2.1 *Soit $f(x) \in \mathbb{F}[x]$ tel que $\overline{f(x)} \neq 0$. Puisque $p(x)$ est irréductible et $p(x)$ n'est pas un facteur de $f(x)$ alors*

$$pqcd(f(x), p(x)) = 1 \in \mathbb{F}^*$$

d'où il existe $a(x)$ et $b(x)$ dans $\mathbb{F}[x]$ tels que $a(x)f(x) + b(x)p(x) = 1$ d'où

$$\overline{a(x)f(x)} + \overline{b(x)p(x)} = \overline{1} \text{ or } \overline{p(x)} = 0.$$

Donc tout élément non nul de K est inversible.Donc K est un corps.

On a $\mathbb{F} \subset \mathbb{F}[x]$ et on considère la restriction à $\mathbb{F}$ de la surjection canonique

$$\begin{aligned} \phi : \mathbb{F} &\to K \\ a &\to \overline{a} \end{aligned}$$

C'est un morphisme injectif d'où $Im(\phi) = \overline{\mathbb{F}}$ est un sous corps de K.

Exemple 1.2.3 *1. Soit $F = \mathbb{R}$ et $p(x) = x^2 - 3x + 2 = (x-1)(x-2)$. Alors $p(x)$ n'est pas irréductible, et donc $Q = \mathbb{R}[x]/(p(x))$ n'est pas un corps.*

2. Soit $F = \mathbb{Q}$ et $p(x) = x^2 - 3$ .nous avons vu que $x^2 - 3$ est irréductible dans $\mathbb{Q}[x]$, et donc $\mathbb{Q}[x]/(p(x))$ est un corps.

1.3 Extension d'un corps fini

Définition 1.3.1 *On dit que K est une **extension** de k si l'on s'est donné un morphisme (nécessairement injectif) $k \to K$. On utilise la notation K/k pour signifier que K est une extension de k. Parfois, on dira aussi que K est un **surcorps** de k.*

Théorème 1.3.1 *Tout corps fini K de caractéristique p est possède p^m éléments oú $m = [K : \mathbb{Z}/p\mathbb{Z}]$ est la dimension de K sur $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration 1.3.1 *Soit $a_1, a_2, ..., a_m$ soit une base pour K sur $p\mathbb{Z}$ Ensuite, chaque élément de K est uniquement exprimable sous la forme $\lambda_1 a_1 + \lambda_2 a_2 + ... + \lambda_K a_K$ avec le λ_i dans $\mathbb{Z}$, et comme il y a p choix pour chaque λ_i , il y a p^m ces expressions tout à fait.*

Propotition 1.3.1
1. *Si K est un corps de caractéristique nulle, alors il existe une unique extension $f : \mathbb{Q} \to K$.*
2. *Si K est un corps de caractéristique $p > 0$, alors il existe une unique extension $f : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \to K$.*

Exemple 1.3.1 *1. $\mathbb{C}$, le corps des nombres complexes, est une extension de $\mathbb{R}$, le corps des nombres réels, lequel est lui-même une extension de $\mathbb{Q}$, le corps des nombres rationnels.*

2. Nous avons vu que $\mathbb{R}[X]/(x^2 + 1)$ est un corps (isomorphe à $\mathbb{C}$) contenant $\mathbb{R}$ comme sous corps, et que $\mathbb{Q}[x]/(x^2 - 3)$ est un corps contenant $\mathbb{Q}$ comme sous corps.

Lemme 1.3.1 *Supposons que F est un corps fini et que K est une extension finie de F, avec $d = [K : F]$. Alors $|K| = |F|^d$*

Définition 1.3.2 ***(Sous-corps engendré)*** *1.Soient K un corps et S une partie de K. L'ensemble des sous-corps de K contenant S est non-vide (car il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K. C'est le plus petit sous-corps contenant S ; on l'appelle le sous-corps engendré par S.*

2.On appelle ***sous-corps premier*** *de K le sous-corps de K engendré par l'élément 1_K. Il est contenu dans tout sous-corps de K.*

3.Soit K/k une extension de corps et soit S une partie de K. L'ensemble des sous-corps de K contenant k et S est non-vide (car

il contient K) et donc l'intersection de tous ces sous-corps est un sous-corps de K, qui est le plus petit sous-corps contenant k et S. On l'appelle le sous-corps ***engendré par*** *S sur k et on le note $k(S)$, ou $k(x_1, ..., x_n)$ si $S = \{x_1, ..., x_n\}$.*

Définition 1.3.3 ***(Extension de type fini)***

1. *On dit queK/k est une* ***extension de type fini*** *si K est engendré comme surcorps de k par un nombre fini d'éléments, c.à.d., s'il existe $x_1, ..., x_n \in K$ tels que $K = k(x_1, ..., x_n)$.*
2. *On dit que K/k est une* ***extension monogène*** *si K est engendré sur k par un élément x, c-à-d., s'il existe $x \in K$ tel que $K = k(x)$.*
3. *Une extension est simple si et seulement si elle est engendrée par un élément.*

Extensions algébriques

Soit E un corps d'extension de F et soit $a \in E$. Toute sous-anneau de E contenant F et contenant a clairement doit contenir a^2, a^3, a^4.... et doit donc contenir tout de la forme $b_0 + b_1 a + ... + b_n a^n$ avec $0 \leq n \in \mathbb{Z}$ et $b_0, b_1, ...b_n \in F$. Autrement dit, il doit contenir tout de la forme $f(a)$ pour $f(x) \in F[x]$.

Définition 1.3.4 *Soit $F[a]$ un sous ensemble de E définie par :*

$$F[a] = \{f(a) \ | \ f(x) \in F[x]\} \ .$$

Tout sous corps S de E qui contient F et aussi a certainement contient $F[a]$ (puisque S est aussi une sous-anneau). Donc, si $u, v \in F[a]$ et $v \neq 0$, il s'ensuite que $uv^{-1} \in S$.

Définition 1.3.5 *Soit $F(a) = \{uv^{-1}/u, v \in F[a]$ et $v \neq 0\}$.*

Théorème 1.3.2 *Soit E un corps d'extension de F et soit $a \in E$.*

- *$F[a]$ est un sous-anneau de E contenant F et a, et tout sous-anneau*

de E contenant F et a contient $F[a]$.
• $F(a)$ est un sous corps de E contenant $F[a]$. Tout sous corps de E contenant F et a contiennent $F(a)$.

Exemple 1.3.2 *:*
Si F est un sous-corps de $\mathbb{R}$ et $0 < a \in \mathbb{R}$ avec $a \notin F$ alors

$$F(a) = F[a] = \{x + y\sqrt{a} \mid x, y \in F\}$$

est un sous corps de $\mathbb{R}$, et est une extension de F de dégrée 2.

Définition 1.3.6 *Soit $k \subset K$ une extension de corps. Un élément $a \in K$ est dit **algébrique** sur k s'il existe un polynôme $P \in k[x]$ non nul tel que $P(a) = 0$. Dans le cas contraire on dit que a est transcendant sur k. L'extension K/k est dit **algébrique** si tous les éléments de K sont algébriques sur k.*

Exemple 1.3.3 — *i est algébrique sur $\mathbb{R}$.*
— *$\mathbb{C}$ est une extension algébrique de $\mathbb{R}$. $\mathbb{R}$ n'est pas une extension algébrique de $\mathbb{Q}$.*

Propotition 1.3.2 *Les extensions finies sont algébriques.*

Corollaire 1.3.1 *Le sous-ensemble A des éléments algébriques de K sur k est un sous- corps de K.*

Démonstration 1.3.2 *Notons que A contient 0 et 1. Soient alors $x, y \in A$ de sorte que . On en déduit alors que les $x^i y^j$ pour $1 \leq i \leq n$ et $1 \leq j \leq m$ engendrent $k[x, y]$ qui est donc de dimension finie sur k. Mais comme $k[x - y]$ et $k[xy]$ sont contenus dans $k[x, y]$, ils sont aussi de dimension finie et donc et sont aussi dans A. On conclut en notant que si x est annulé par P alors $1/x$ est annulé par le polynôme $x^{deg(p)}p(1/x)$.*

Éléments primitifs

Lorsque vous travaillez avec un corps fini, il faut pouvoir ajouter et multiplier aussi simplement que possible. Rappelons que l'ensemble $\mathbb{F}_q^*$ *de l'éléments non nuls dans* $\mathbb{F}_q$ *est un groupe.*

Corollaire 1.3.2 *Le groupe* $\mathbb{F}_q^*$ *est cyclique d'ordre* $q-1$ *sous la multiplication de* $\mathbb{F}_q$ *.*

Définition 1.3.7 *Chaque générateur* λ *de* $\mathbb{F}_q^*$ *est appelé* ***élément primitif*** *de* $\mathbb{F}_q$*, et donc*

$$\mathbb{F}_q = \{0, 1 = \lambda^0, \lambda, \lambda^2, ..., \lambda^{q-2}\}$$

et $\lambda^i = 1$ *si et seulement si* $(q-1)|i$ *.*

Lorsque les éléments non nuls de un corps fini s'exprime en puissances de λ *, la multiplication dans le corps s'effectue facilement selon la règle*

$$\lambda^i \lambda^j = \lambda^{i+j} = \lambda^s$$

Où $0 \leq s \leq q-2$ et $i + j \equiv s (\text{mod } q-1)$.

Soit λ *un élément primitif de* $\mathbb{F}_q$ *. Alors* $\lambda^{q-1} = 1$ *par définition. D'où* $(\lambda^i)^{q-1} = 1$ *pour* $0 \leq i \leq q-2$ *montrant que les éléments de* $\mathbb{F}_q^*$ *sont des racines de* $x^{q-1} - 1 \in \mathbb{F}_q[x]$ *et donc de* $x^q - x$ *. Comme 0 est une racine de* $x^q - x$ *, nous voyons maintenant que les éléments de* $\mathbb{F}_q$ *sont précisément les racines de* $x^q - x$ *donnant cet important théorème.*

Théorème 1.3.3 *Les éléments de* $\mathbb{F}_q$ *sont précisément les racines de* $x^q - x$*.*

Dans tout groupe cyclique fini G d'ordre n avec générateur g, les générateurs de G sont précisément les éléments g^i où $gcd(i, n) = 1$. On laisse $\phi(n)$ soit le nombre d'entiers i avec $1 \leq i \leq n$ tels que $gcd(i, n) = 1$; ϕ est appelé fonction d'Euler ϕ ,Il y a donc $\phi(n)$ générateurs de G.

Théorème 1.3.4 *Soit λ un élément primitif de $\mathbb{F}_q$*

1. *Il y a $\phi(q-1)$ éléments primitifs dans $\mathbb{F}_q$; ce sont les éléments λ^i . où $pgcd(i, q-1) = 1$*
2. *Pour tout d où $d|(q-1)$, il y a $\phi(d)$ éléments dans $\mathbb{F}_q$ d'ordre d ; Voici les éléments $\lambda^{(q-1)i/d}$ où $gcd(i, d) = 1$.*

Lemme 1.3.2 *Le nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$ est égal à $\phi(d)$.*

1.4 Construction de corps finis

Nous avons montré que pour tout corps $\mathbb{F}$ nous pouvons construire un corps K contenant $\mathbb{F}$ comme sous corps.

Théorème 1.4.1 *Soit $\mathbb{F}$ un corps et $p(x) = c_0 + c_1x + ... + c_mx^m \in \mathbb{F}[x]$ un polynôme irréductible de degré $m \geq 1$. Alors le corps $K = \mathbb{F}[x]/(p(x))$ peut être représenté comme*

$$K = \{a_0 + a_1t + ... + a_{m-1}t^{m-1}/a_0, ..., a_{m-1} \in \mathbb{F}; p(t) = 0\}$$

Exemple 1.4.1 *L'anneau quotient $K = \mathbb{R}[x]/(x^2+1)$ est un corps isomorphe à $\mathbb{C}$. En effet, Puisque le polynôme $p(x) = x^2 + 1$ est irréductible sur $\mathbb{R}$, l'anneau quotient K est un corps. K peut être représenté par*

$$K = \{a_0 + a_1t/a_0, a_1 \in \mathbb{R}\}$$

où t vérifie $t^2 + 1 = 0$. On vérifie facilement que l'application $f : K \to \mathbb{C}$ définit par $f(a + bt) = a + ib$ est un isomorphisme de corps.

Pour construire un corps d'ordre p^m , on considère le corps $\mathbb{Z}_p$ et $p(x) \in \mathbb{Z}p[x]$ un polynôme irréductible de degré m. Soit $p(x) = c_0+c_1x+...+c_mx^m$ alors le corps $K = \mathbb{Z}p[x]/p(x)$ peut être représenté comme

$$K = \{a_0 + a_1t + ... + a_{r-1}t^{r-1}|a_i \in \mathbb{Z}_p, p(t) = 0\}.$$

Corollaire 1.4.1 *Si $n = p^r$ où p un nombre premier et r un entier > 0. Alors il existe un corps fini $\mathbb{F}_{p^r}$ d'ordre p^r donné par*

$$\mathbb{F}_{p^r} = \{a_0 + a_1 t + ... + a_{r-1} t^{r-1} | a_i \in \mathbb{Z}_p, p(t) = 0\}$$

où $p(x) \in \mathbb{Z}_p[x]$ est un polynôme irréductible unitaire de degré r.

Exemple 1.4.2 *Cherchons un corps à 9 éléments. On a $9 = 3^2$, on a besoin d'un polynôme irréductible de degré 2 dans $\mathbb{Z}_3[x], x^2 + 1$ l'est.*

$$\mathbb{F}_9 = \{a + bt | a, b \in \mathbb{Z}_3, t^2 + 1 = 0\}$$

d'où

$$\mathbb{F}_9 = \{0, 1, 2, t, 1 + t, 2 + t, 2t, 1 + 2t, 2 + 2t\}$$

Dans $\mathbb{F}_9$ on a $(1 + t)(1 + 2t) = 1 + t + 2t + 2t^2 = 1 + 2t^2 = 2$

Exemple 1.4.3 *Le polynôme $f(x) = x^4 + x^3 + 1$ est irréductible sur $\mathbb{F}_2$, alors l'éléments de $\mathbb{F}_{16} = \mathbb{F}_2[x]/(f(x))$ sont donnés par :*

$$\mathbb{F}_{16} = \{a + bt + ct^2 + dt^3 | a, b, c, d \in \mathbb{Z}_2, t^4 + t^3 + 1 = 0\}$$

*Donc les éléments de $\mathbb{F}_{16}$ sont :*0,1, α, $\alpha + 1$,α^2,$\alpha^2 + 1$,$\alpha^2 + \alpha$,$\alpha^2 + \alpha + 1$,α^3,$\alpha^3 + 1$, $\alpha^3 + \alpha$,$\alpha^3 + \alpha + 1$,$\alpha^3 + \alpha^2$,$\alpha^3 + \alpha^2 + 1$,$\alpha^3 + \alpha^2 + \alpha$,$\alpha^3 + \alpha^2 + \alpha + 1$.

On a $f(\alpha) = \alpha^4 + \alpha^3 + 1 = 0$, ce qui implique que $\alpha^4 = \alpha^3 + 1$. Donc $\alpha^5 = \alpha\alpha^4 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$, $\alpha^6 = \alpha\alpha^5 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$,et ainsi de suite on obtient la table :

$0 = 0$	$\alpha^3 = \alpha^3$
$1 = \alpha^0 = 1$	$\alpha^3 + 1 = \alpha^4$
$\alpha = \alpha$	$\alpha^3 + \alpha = \alpha^{10}$
$\alpha + 1 = \alpha^3$	$\alpha^3 + \alpha + 1 = \alpha^5$
$\alpha^2 = \alpha^2$	$\alpha^3 + \alpha^2 = \alpha^{14}$
$\alpha^2 + 1 = \alpha^6$	$\alpha^3 + \alpha^2 + 1 = \alpha^{11}$
$\alpha^2 + \alpha = \alpha^4$	$\alpha^3 + \alpha^2 + \alpha = \alpha^8$
$\alpha^2 + \alpha + 1 = \alpha^5$	$\alpha^3 + \alpha^2 + \alpha + 1 = \alpha^6$

1.5 polynômes minimaux et classes cyclotomiques

Définition 1.5.1 *Soit $\mathbb{F}_{q^t}$ une extension fini de $\mathbb{F}_q$.soit $\alpha \in \mathbb{F}_{q^t}$. 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 $M_\alpha(x)$.*

Exemple 1.5.1 *Soit α une racine du polynôme $1 + x + x^2 \in \mathbb{F}_2[x]$. C'est clair que les deux polynômes linéaires x et $x + 1$ ne sont pas des polynômes minimaux de α. Par conséquent, $1 + x + x^2$ est un polynôme minimal de α.*

Puisque $1+(1+\alpha)+(1+\alpha)^2 = 1+1+\alpha+1+\alpha^2 = 1+\alpha+\alpha^2 = 0$ et $1 + \alpha$ n'est pas une racine de x ou $1 + x$, $1 + x + x^2$ est aussi un polynôme minimal de $1 + \alpha$.

Propotition 1.5.1 *Soit $\alpha \in \mathbb{F}_{q^t}$, soit d un entier positif non nul. Le degré du polynôme minimal $M_\alpha(x)$ de α 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 $\mathbb{F}^*_{q^t}$ est le plus petit entier positif non nul l tel que $\alpha^l = 1$.

Lemme 1.5.1 *Soit $\alpha \in \mathbb{F}_{q^t}$. Soit l l'ordre de α. 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 $d = ord_l(q)$.*

Corollaire 1.5.1 *Soit $\alpha \in \mathbb{F}_{q^t}$. Soit l l'ordre de α. Alors :*

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

Où $l \in \{1, 2, ..., q^t - 1\}$

Propotition 1.5.2 *Soit* $\alpha \in \mathbb{F}_{q^t}$. *Soit* l *l'ordre de* α. *Alors :*

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

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

Supposons maintenant que λ est un élément primitif de $\mathbb{F}_{q^t}$. Alors $\alpha = \lambda^s$ pour certains s. D'où $\alpha^{q^r} = \alpha$ si et seulement si $\lambda^{sq^r - s} = 1$. et on a, $sq^r \equiv s(\mod q^t - 1)$. Sur cette base, nous avons la définition de la classe q-cyclotomique ;

Définition 1.5.2 *La classe q-cyclotomique de* s *modulo* $q^t - 1$ *est l'ensemble*

$$C_s = \{s, sq, ..., sq^{r-1}\}(\mod q^t - 1)$$

où r *est le plus petit entier positif tel que* $sq^r \equiv s(\mod q^t - 1)$.

Exemple 1.5.2 *Les classes 2-cyclotomique modulo 15 sont*

$$C_0 = \{0\},\ C_1 = \{1, 2, 4, 8\},\ C_3 = \{3, 6, 12, 9\},$$

$$C_5 = \{5, 10\},\ C_7 = \{7, 14, 13, 11\}.$$

Définition 1.5.3 *Le polynôme minimal* $M_\alpha(x)$ *d'un élément primitif* α *, s'appelle polynôme primitif.*

Théorème 1.5.1 *Soit* α *une élément primitive de* $\mathbb{F}_{q^m}$.*Alors le polynôme minimale de* α^i *est*

$$M^{(i)}(x) = \prod_{j \in C_i} (x - \alpha^j).$$

Exemple 1.5.3 *Soit α une racine du $2 + x + x^2 \in \mathbb{F}_3[x]$; i.e*

$$2 + \alpha + \alpha^2 = 0$$

Alors le polynôme minimal du α et α^3 est $2 + x + x^2$.
Le polynôme minimal du α^2 est

$$M^{(2)}(x) = \prod_{j \in C_2} (x - \alpha^j) = (x - \alpha^2)(x - \alpha^6) = \alpha^8 - (\alpha^2 + \alpha^6)x + x^2.$$

Nous savons que $\alpha^8 = 1$ comme $\alpha \in \mathbb{F}_9$. Pour obtenir $M^{(2)}(x)$, nous devons simplifier $\alpha^2 + \alpha^6$. Et on a $\alpha^2 + \alpha^6 = (1 - \alpha) + (1 - \alpha)^3 = 2 - \alpha - \alpha^3 = 2 - \alpha - \alpha(1 - \alpha) = 2 - 2\alpha + \alpha^2 = 0$. Par conséquent, le polynôme minimal de α^2est $1 + x^2$.de la même manière, on peut obtenir le polynôme minimal $2 + 2x + x^2$ of α^5.

Corps de décomposition

Définition 1.5.4 *Soit $q \in K[X]$ un polynôme unitaire, et $f : K \to L$ une extension. On dit que L est un corps de décomposition de q si et seulement si :*
a) q est scindé dans L.c'est-à-dire, en notant $n = \deg(q)$ et en appelant c le coefficient de x^n dans q.qu'il existe des $\alpha_1, ..., \alpha_n$ dans L tels que

$$q(x) = c \prod_{i=1}^{n} (x - \alpha_i)$$

b) l'extension L est engendrée par les racines de q.

Exemple 1.5.4 *$\mathbb{F}_2$ est un corps de décomposition de $x^2 + x + 1$.*

Théorème 1.5.2 *Soit $f(x) \in F_q[x]$ un polynôme irréductible de degré d, et soit α n'importe quelle racine de $f(x)$.Alors le corps de décomposition de $f(x)$ est*

$$Split(f) = F_q(\alpha) = F_{q^d}$$

En particulier, le corps de décomposition de $f(x)$ a un degré d sur F_q.

Corollaire 1.5.2 *Soit $f(x) \in F_q[x]$ un polynôme irréductible.Alors toutes les racines de $f(x)$ dans $Split(f)$ ont le même ordre multiplicatif.*

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

Racines de l'unité

Notons le corps de décomposition de $x^n - 1$ sur $\mathbb{F}_q$ par $\mathbb{F}_{q^m}$, Le polynôme $x^n - 1$ n'a pas racines multiples dans n'importe quelle extension de $\mathbb{F}_q$. Par conséquent, $x^n - 1$ a des racines distincts dans son corps de décomposition $\mathbb{F}_{q^m}$. Le corps $\mathbb{F}_{q^m}$ s'appelle aussi le corps des racines n-ièmes de l'unité sur $\mathbb{F}_q$.

Corollaire 1.6.1 *Si $\mathbb{F}_{q^m}$ est le corps de décomposition pour $x^n - 1$ sur $\mathbb{F}_q$, alors m est le plus petit entier positif pour lequel $n \mid q^m - 1$, c'est-à-dire, m est le plus petit entier positif pour lequel $q^m \equiv 1 \mod n$. Autrement dit, m est l'ordre de $q \mod n$, que nous noterons $ord_n(q)$.*

Définition 1.6.1 *On appelle racine n-ième de l'unité sur $\mathbb{F}_q$, un élément de $\mathbb{F}_{q^m}$ dont l'ordre divise n, on appelle racine n-ième 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 de l'unité sur $\mathbb{F}_q$ est un élément primitif de $\mathbb{F}_{q^m}$

Les racines n-ièmes de l'unité sur $\mathbb{F}_q$ forment un sous-groupe de 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-ième de l'unité sur $\mathbb{F}_q$.D'ailleurs, $(\beta^{-1})^n = (\beta^n)^{-1} = 1$. 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 u l'entier tel que $un = q^m - 1$. Soit α un élément primitif de $\mathbb{F}_{q^m}$. Alors $\beta = \alpha^u$ est une racine n-ième primitive de l'unité sur $\mathbb{F}_q$,

car l'ordre de α^u est égal à $\frac{q^m-1}{(q^m-1,u)} = \frac{un}{(un,u)} = n$.Donc β est un générateur de ce sous-groupe qui est d'ordre 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

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

Soit γ une racine n-ième 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 $\mathbb{F}_q$.

D'après le théorème 1.5.1 On peut déduire :

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

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

Cas général Prenons maintenant le cas général où n et $s \leq 0$ (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

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

et donc

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

ainsi,

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

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

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

où β est une raciner-iéme primitive de l'unité sur $\mathbb{F}_q$ et j parcourt un ensemble de représentants des classes cyclotomique modulo r sur $\mathbb{F}_q$.

Exemple 1.6.1 *Considérons le polynôme*

$$h_7(x) = x^7 - 1$$

sur $\mathbb{F}_2$. *On a* $n = 7$ *et* $q = 2$. *Puisque* $s = ord_7(2) = 3$, *le corps de décomposition pour* $h_7(x)$ *est* $\mathbb{F}_{q^s} = \mathbb{F}_8$. *Pour les classes cyclotomique modulo 7 on a :*

$C_0 = \{0\}$
$C_1 = \{1, 2, 4\} = C_2$
$C_3 = \{3, 5, 6\}$

Les trois polynômes minimaux sont :

$m_0(x) = (x - 1)$
$m_1(x) = \prod_{i \in C_1} (x - \alpha^i) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$
$m_3(x) = \prod_{i \in C_3} (x - \alpha^i) = (x - \alpha^3)(x - \alpha^5)(x - \alpha^6)$

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

Pour déterminer les coefficients binaire de $m_1(x)$ et $m_3(x)$, il faut faire des calculs dans $\mathbb{F}_8$, nous considérons un polynôme binaire de degré 3 irréductible sur $\mathbb{F}_2$, par exemple $f(x) = x^3 + x + 1$ si α une 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 ;

$$\begin{aligned} m_1(x) &= (x - \alpha)(x - \alpha^2)(x - \alpha^4) \\ &= x^3 + (\alpha + \alpha^2 + \alpha^4)x^2 + (\alpha^3 + \alpha^5 + \alpha^6)x + \alpha^7 \\ &= x^3 + x + 1 \end{aligned}$$

Et on trouve de manière analogue que

$$m_3(x) = x^3 + x^2 + 1$$

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

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

Exemple 1.6.2 *Considérons le polynôme*

$$h_{13}(x) = x^{13} - 1$$

sur $\mathbb{F}_3$. On a $n = 13$ et $q = 3$. Puisque $s = ord_{13}(3) = 3$, le corps de décomposition pour $h_7(x)$ est $\mathbb{F}_{q^s} = \mathbb{F}_{27}$. Pour les classes cyclotomique modulo 7 on a :

$$C_0 = \{0\},\ C_1 = \{1, 3, 9\}, C_2 = \{2, 6, 18\},$$

$$C_4 = \{4, 12, 10\}, C_5 = \{5, 15, 19\}, C_7 = \{7, 21, 11\},$$

$$C_8 = \{8, 24, 20\}, C_{13} = \{13\}, C_{14} = \{14, 16, 22\}, C_{17} = \{17, 25, 23\}.$$

nous connaissons tous les classes cyclotomiques de 3 modulo 26 contenant des multiples de 2. Par conséquent, On obtient

$$M^{(0)}(x) = 2 + x,$$

$$M^{(2)}(x) = \prod_{j \in C_2} (x - \alpha^j) = (x-\alpha^2)(x-\alpha^6)(x-\alpha^18) = 2+x+x^2+x^3,$$

$$M^{(4)}(x) = \prod_{j \in C_4} (x - \alpha^j) = (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10}) = 2+x^2+x^3,$$

$$M^{(8)}(x) = \prod_{j \in C_8} (x - \alpha^j) = (x-\alpha^8)(x-\alpha^{20})(x-\alpha^{24}) = 2+2x+2x^2+x^3,$$

$$M^{(14)}(x) = \prod_{j \in C_{14}} (x - \alpha^j) = (x-\alpha^{14})(x-\alpha^{16})(x-\alpha^{22}) = 2+2x+x^3.$$

on obtient la factorisation de $x^{13} - 1$ *sur* $\mathbb{F}_{13}$ *en polynômes unitaires irréductibles :*

$$\begin{aligned} x^{13} - 1 &= M^{(0)}(x)M^{(2)}(x)M^{(4)}(x)M^{(8)}(x)M^{(14)}(x) \\ &= (2+x)(2+x+x^2+x^3)(2+x^2+x^3)(2+2x+2x^2+x^3)(2+2x+x^3). \end{aligned}$$

Chapitre 2

Les codes

Dans ce chapitre on va présenter les définitions et le principe général des codes, puis on passera a'un cas particulier des codes qui est les codes linéaires et plus précisément on va ce concentrer sur les codes cycliques.

2.1 Code

Définition 2.1.1 *Soit $\mathcal{A} = \{a_1, a_2, ..., a_q\}$ un ensemble fini, que nous appelons* ***un alphabet****. Une* ***chaîne****, ou un* ***mot****, sur l'alphabet $\mathcal{A}$ est une séquence d'éléments de $\mathcal{A}$. Nous allons généralement écrire des mots sous la forme*

$$a = a_{i_1} a_{i_2} ... a_{i_k}$$

Définition 2.1.2 *Soit $\mathcal{A}$ une* ***alphabet*** *de cardinal q. M, n deux entiers strictement positifs. On appelle* ***code*** *C sur l'alphabet $\mathcal{A}$ de longueur n toute partie $C \subset \mathcal{A}^n$ de cardinal $Card(C) = M$.*
Un code $C \subset \mathcal{A}^n$ est dit ***q-aire*** *si $C = ImE$ pour une application injective*

$$E : \mathcal{A}^k \to \mathcal{A}^n$$

L'élément $E(u)$, pour un u de $\mathcal{A}^k$ est appelé ***un mot code****, n est sa longueur. Dans ce cas $M = q^k$,*

On peut aussi considérer l'ensemble de toutes les images pour construire le code

$$C = \{y \in \mathcal{A}^n \ : y = E(u); u \in \mathcal{A}^k\}.$$

Exemple 2.1.1 *Considère* $C = \{c_0, c_1, c_2, c_3\}$ *avec*

$$c_0 = (00000), c_1 = (10110), c_2 = (01011), c_3 = (11101).$$

C'est un code de longueur 5 sur l'alphabet $\mathcal{A} = \mathbb{F}_2 = \{0, 1\}$.

Distance de Hamming

Rappelons tout d'abord les caractéristiques d'un distance d entre x et y :

$$\begin{array}{ll} d(x,y) > 0\,; & d(x,y) = 0 \iff x = y \\ d(x,y) = d(y,x)\,; & d(x,y) \leq d(x,z) + d(z,y) \end{array}$$

Définition 2.1.3 *Soit* $\mathcal{B}$ *un alphabet.On définit la distance de Hamming* d *sur les lettres de* $\mathcal{B}$ *par :*

$$d(x,y) = \begin{cases} 1 & si \quad x \neq y \\ 0 & si \quad x = y \end{cases}$$

pour $x, y \in \mathcal{B}$ *.Soit* $n \in \mathbb{N}$ *et* $\mathcal{B}^n = \{x = (x_1, x_2, ..., x_n) : 1 \leq i \leq n; x_i \in \mathcal{B}\}$ *l'ensemble des mots à n lettres .On définit* d_H *la distance de Hamming sur les mots à n lettre comme :*

$$d_H(x,y) = \sum_{i=1}^{n} d(x_i, y_i)$$

pour $x, y \in \mathcal{B}^n$ *.*

Propotition 2.1.1 *La distance de Hamming est bien une distance.*

Exemple 2.1.2 *Si* $x = 10112$ *et* $y = 20110$, *donc* $d_H(x, y) = 2$.

Définition 2.1.4 ***(Poids de Hamming)*** *Le poids d'un mot* $x \in \mathcal{B}^n$ *,noté* $w(x)$ *définit comme la distance de* x *au mot* $\underline{0}$ *,i,e*

$$w(x) = d_H(\underline{0}, x)$$

A partir de la distance de Hamming sur les mots, il est possible de définir la boule de centre x *et de rayon* e *noté* $B_e(x)$ *par :*

$$B_e(x) = \{z, z \in B^n, d_H(x, z) \leq e\}$$

pour $e \in \mathbb{N}, x \in \mathcal{B}^n$.

Définition 2.1.5 *On appelle distance minimal d'un code* C *la quantité :*

$$d_H(C) = min\{d_H(x, y) \ : x, y \in C, x \neq y\}.$$

Et poids minimal d'un code C *la quantité :*

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

Exemple 2.1.3 *Pour le code de l'exemple précédent, on a :*

$$\begin{aligned} d_H(x, y) &= d_H(01110, 10101) = 4 \\ d_H(x, z) &= d_H(01110, 11011) = 3 \\ d_H(y, z) &= d_H(10101, 11011) = 3 \end{aligned}$$

la distance minimal de C *est* $d_H(C) = 3$, *et son poids minimal est* $w(C) = 3$.

2.2 Code linéaire

Définition 2.2.1 *Un code* C *est dit linéaire sur* $\mathbb{F}_q$, *si* C *est un sous-espace vectoriel de* $\mathbb{F}_q^n$ *.Autrement dit,* C *vérifie*

$$\forall u, v \in C; u + v \in C$$
$$\forall u \in C, \forall a \in \mathbb{F}_q; a.u \in C$$

• *La dimension de C sur $\mathbb{F}_q$ est appelée la dimension du code C et est noté $dimC$.*

Notation : *Un code linéaire de longueur n, dimension k, et distance minimale d sera noté un code $[n, k, d]$ (ou $[n, k]$ si d n'est pas connue ou elle n'est pas importante).*

Théorème 2.2.1 *Si C est un code linéaire de dimension k, alors $|C| = q^k$, i.e. $\dim(C) = \log_q |C|$.*

Exemple 2.2.1 *$C = \{00000000, 11110000, 00001111, 11111111\}$, Le code est un sous espace vectoriel de $\mathbb{F}_2^8$ de dimension $k = 2$ C'est un code linéaire de paramètres $[n = 8, k = 2, d = 4]$.*

Théorème 2.2.2 *La distance minimale d'un code linéaire C est égale à son poids minimal.*

Matrice génératrice d'un code linéaire

Définition 2.2.2 *Le code C peut être défini au moyen d'une matrice G à k lignes et n colonnes appelée matrice génératrice dont les lignes forment une base de C.*

Soient $\{v_1, v_2, ..., v_k\}$ les vecteurs lignes de G. Tout élément x de C peut être exprimé comme une unique combinaison linéaire de ces lignes, i.e $x = \sum_{i=1}^{k} a_i v_i$ pour des a_i dans $\mathbb{F}_q$. Donc
$C = \{x/x = a.G, a \in \mathbb{F}_q\}$.

Exemple 2.2.2 *Considérons le code binaire avec la matrice génératrice*

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

Ce code peut encoder des symboles source à partir de $\mathbb{F}_2^3$. *En particulier, pour chaque* $x = (x_1, x_2, x_3) \in \mathbb{F}_2^3$, *on associe le mot de code*

$$[x_1x_2x_3]\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} = (x_1 + x_3, x_1 + x_2, x_2 + x_3, x_2)$$

Les mots du code sont $\{0000, 1010, 0111, 1100, 1101, 0110, 1011, 0001\}$. *Ainsi, le code est de paramètre* $[8, 3, 1]$ *et* $|C| = q^k = 2^3 = 8$

2.3 Dual d'un code linéaire

les codes duaux vont jouer un rôle important dans la théorie des codes linéaires.

Définition 2.3.1 *le code dual de* C *noté par* $C^\perp$ *est :*

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

où $\langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$ *est le produit scalaire de* x *par* y.

Théorème 2.3.1
1) Si G *est une matrice génératrice pour* C, *alors*

$$C^\perp = \{x \in F_q^n \quad | \quad xG^t = 0\}.$$

2) Le dual $C^\perp$ *d'un* $[n, k]$*-code linéaire est un* $[n, n-k]$*-code linéaire.*
3) Pur tout code linéaire C, *on a* $(C^\perp)^\perp = C$.

Remarque 2.3.1 *Si* C *et* $C^\perp$ *sont équivalents, le code* C *sera dit auto dual.*

Matrice de Contrôle

Définition 2.3.2 *La matrice de controle* H *d'un code linéaire* C *est la matrice génératrice du code dual* $C^\perp$

2.4 Codes cycliques

Définition 2.4.1 *Un code linéaire $C \subset \mathbb{F}_q^n$ est dit cyclique s'il vérifie la propriété suivante :*

$$\textit{si } x_1...x_n \in C, \textit{ alors } x_n x_1...x_{n-1} \in C.$$

Exemple 2.4.1 *Le code $C = \{000, 110, 011, 101\}$ est un code cyclique.*

Représentation polynomiale

Nous supposons que $pgcd(n, q) = 1$ et on notera $(x^n - 1)$ l'idéal de $\mathbb{F}_q[x]$ engendré par $x^n - 1$. Alors, tout élément de $R_n = \mathbb{F}_q[x]/(x^n - 1)$ peut être représenté par des polynômes de degré inférieur à n (ou le polynôme nul), et cet anneau est ainsi isomorphe à $\mathbb{F}_q^n$ comme $\mathbb{F}_q$-espace vectoriel.
L'isomorphisme est donné par

$$c_0 c_1 ... c_{n-1} \to c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

Cet isomorphisme permet de considérer les éléments de $\mathbb{F}_q[x]/(x^n - 1)$ comme des vecteurs de $\mathbb{F}_q^n$ ou comme des polynômes de degré $< n$ modulo $x^n - 1$.

Exemple 2.4.2 *Le code $C = \{000, 110, 011, 101\}$ correspond aux polynômes*
$0,\ 1 + x,\ x + x^2,\ 1 + x^2$ *pris modulo $x^3 - 1$. Sa représentation polynomiale est donc $C = \{0, 1 + x, x + x^2, 1 + x^2\}$.*

Polynôme générateur d'un code cyclique

Théorème 2.4.1 *Le code linéaire C de longueur n sur le corps $\mathbb{F}_q$ est cyclique si et seulement si C est un idéal de $\mathbb{F}_q[x]/(x^n - 1)$.*

Preuve 2.4.1 *C est un idéal de $\mathbb{F}_q[x]/(x^n - 1)$ et $(a_0, ..., a_{n-1}) \in C$, alors*

$$x.(a_0, ..., a_{n-1}) = (a_{n-1}, a_0, ..., a_{n-2}) \in C \ .$$

Inversement, si C est cyclique, pour tout $a(x) \in C, xa(x) \in C, x^2a(x) \in C$ et ainsi de suite, donc $b(x)a(x) \in C$ et C est un idéal.

L'anneau $\mathbb{F}_q[x]$ est principal, donc tous les idéaux de l'anneau $\mathbb{F}_q[x]/(x^n - 1)$ sont principaux. En particulier, tout idéal non nul est engendré par un polynôme g(x) de plus bas degré qu'il contient :

$$C = \langle 1.g(x), x.g(x), x^2.g(x), ..., x^{k-1}.g(x) \rangle$$

Théorème 2.4.2 *Soit C un idéal dans R_n, c'est-à-dire un code cyclique de longueur n.*

1. Il existe un polynôme unique $g(x)$ de degré minimum dans C. Ce polynôme engendré C, c'est-à-dire $C = \langle g(x) \rangle$, et il appelé polynôme générateur pour C.

2. Le polynôme générateur $g(x)$ divise $x^n - 1$.

3. Si $\deg(g(x)) = r$, alors C a la dimension $n - r$ et

$$C = \langle g(x) \rangle = \{r(x)g(x) \mid \deg(r(x)) < n - r\}.$$

Preuve 2.4.2 *1. Supposons que C contienne deux polynômes distincts $g_1(x)$ et $g_2(x)$ de degré minimum r. Alors leur différence $g_1(x) - g_2(x)$ serait un polynôme non nul en C de degré inférieur à r, qui n'est pas possible. Par conséquent, il existe un polynôme unique $g(x)$ de degré r dans C. Puisque $g(x) \in C$ et C est un idéal, nous avons $\langle g(x) \rangle \subset C$. Par contre, supposons que $p(x) \in C$, et soit*

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

où $\deg(r(x)) < r$. Alors $r(x) = p(x) - q(x)g(x) \in C$ a un degré inférieur à r, ce qui n'est possible que si $r(x) = 0$. Par conséquent, $p(x) = q(x)g(x) \in \langle g(x) \rangle$, et donc $C \subset \langle g(x) \rangle$. Ainsi, $C = \langle g(x) \rangle$.

2. Diviser $x^n - 1$ *par* $g(x)$ *donne*

$$x^n - 1 = q(x)g(x) + r(x)$$

où $\deg(r(x)) < r$. *Puisque dans* $R_n = x^n - 1 = 0 \in C$, *nous voyons que* $r(x) \in C$, *et donc* $r(x) = 0$, *qui montre que* $g(x) \mid x^n - 1$.

3. L'idéal généré par $g(x)$ *est*

$$\langle g(x) \rangle = \{f(x)g(x) \mid f(x) \in R_n\}$$

avec le modulo de réduction habituel $x^n - 1$, *et nous devons montrer qu'il suffit de restreindre* $f(x)$ *à des polynômes de degré inférieur à* $n - r$. *Nous avons vu que* $g(x) \mid x^n - 1$, *et donc* $x^n - 1 = h(x)g(x)$. *Pour un polynôme* $h(x)$ *de degré* $n - r$. *Divisons* $f(x)$ *par* $h(x)$

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

où $\deg(r(x)) < n - r$. *Alors*

$$f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n - 1) + r(x)g(x)$$

et donc $f(x)g(x) = r(x)g(x)$ *dans* R_n *qui est ce que nous voulions montrer. Cela montre également que l'ensemble*

$$\{g(x), xg(x), ..., x^{n-r-1}g(x)\}$$

s'étend sur C, et comme il est linéairement indépendant, il forme une base pour C. Par conséquent $\dim(C) = n - r$.

Exemple 2.4.3 *Le code* $C = \{0, 1 + x, x + x^2, 1 + x^2\}$ *est engendré par*
$g(x) = 1 + x$ *dans* $\mathbb{F}_2[x]/(x^3 - 1)$.

Théorème 2.4.3 *Soit* $g(x) = g_0 + g_1x + ... + g_rx^r$ *le générateur d'un code cyclique C de longueur n. alors* $g_0 \neq 0$ *et C a une matrice génératrice donnée par :*

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_r \end{bmatrix}.$$

Remarque 2.4.1 *Il est important de noter qu'un code cyclique C peut être généré par des polynômes autre que le polynôme générateur.*

Exemple 2.4.4 *Considérons le code cyclique $C = \langle 1 + x \rangle$ dans R_3, alors* $\dim(C) = 3 - 1 = 2$ *et que C contient les mots de code*

$$0, \;\; 1 + x, \;\; x(1 + x) = x + x^2, \;\; (1 + x)(1 + x) = 1 + x^2$$

donc

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

notez que

$$\langle 1 + x^2 \rangle = \{f(x)(1 + x^2) \mid f(x) \in R_3\} = C$$

Donc C est généré également par le polynôme $1 + x^2$.

Théorème 2.4.4 *Un polynôme unitaire $p(x) \in R_n$, est le polynôme générateur d'un code cyclique si et seulement si $p(x) \mid x^n - 1$.*

Preuve 2.4.3 *Nous avons déjà établi une implication.Quant à l'inverse, supposons que $p(x) \mid x^n - 1$, et soit $g(x)$ le polynôme générateur pour $C = \langle p(x) \rangle$. Supposons que $p(x) \neq g(x)$. Puisque $p(x)$ et $g(x)$ sont tous les deux unitaires, nous devons avoir* $\deg(p(x)) > \deg(g(x))$.
Par hypothèse,

$$x^n - 1 = p(x)f(x) \tag{2.1}$$

pour un polynôme $f(x)$. De plus, puisque $g(x) \in \langle p(x) \rangle$, nous avons

$$g(x) \equiv a(x)p(x)$$

pour certains $a(x) \in R_n$. *Multipliant les deux côtés de ceci par* $f(x)$ *et en utilisant* (1) *donne*

$$g(x)f(x) \equiv a(x)p(x)f(x) \equiv a(x).(x^n - 1) \equiv 0$$

Mais $\deg(g(x)f(x)) < \deg(p(x)f(x)) = n$, *et donc* $g(x)f(x) = 0$, *ce qui n'est pas possible. Donc* $p(x) = g(x)$.

Exemple 2.4.5 *Nous avons vu que* x^9-1 *facteurs sur* $\mathbb{F}_2$ *en facteurs irréductibles comme suit*

$$x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

Donc, il y a $2^3 = 8$ *codes cycliques dans* R_9. *Par exemple, le code cyclique* $C_1 = \langle x^6+x^3+1\rangle$ *a une dimension* $9-6 = 3$ *et une matrice génératrice*

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Exemple 2.4.6 *Sur* $\mathbb{F}_2$ *on a* $x^7-1 = (x+1)(x^3+x^2+1)(x^3+x+1)$ *alors les codes cycliques de longueur* 7 *sur* $\mathbb{F}_q$ *sont :*

$\langle 1\rangle = R_n$,
$\langle (x+1)\rangle$,
$\langle (x^3+x+1)\rangle$,
$\langle (x^3+x^2+1)\rangle$,
$\langle (x+1)(x^3+x+1)\rangle$,
$\langle (x+1)(x^3+x^2+1)\rangle$,
$\langle (x^3+x+1)(x^3+x^2+1)\rangle$,
$\langle 0\rangle = \{0\}$.

Exemple 2.4.7 *Le but est de déterminer tous les codes ternaires de longueur* 4 *et leurs générateurs. La factorisation de* $x^4 - 1$ *sur* $\mathbb{F}_3$ *a la forme*

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

Par conséquent, il y a $2^3 = 8$ *diviseurs de* $x^4 - 1$ *et chacun génère un code cyclique.*

Polynôme générateur	*Matrice génératrice*
1	I_4
$x-1$	$\begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix}$
$x+1$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
x^2+1	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$
$(x-1)(x+1) = x^2 - 1$	$\begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{bmatrix}$
$(x-1)(x^2+1) = x^3 - x^2 + x - 1$	$\begin{bmatrix} -1 & 1 & -1 & 1 \end{bmatrix}$
$(x+1)(x^2+1)$	$\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$
$x^4 - 1 = 0$	$\begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix}$

Polynôme de contrôle d'un code cyclique

Puisque le polynôme générateur $g(x)$ de degré r d'un $[n, n-r]$-code cyclique dans R_n divise $x^n - 1$, nous avons

$$x^n - 1 = g(x)h(x)$$

où $h(x)$ est un polynôme de degré $n - r$, appelé le polynôme de

contrôle de C. Cette terminologie est expliquée par le théorème suivant.

Théorème 2.4.5 *Soit $h(x)$ le polynôme de contrôle pour un code cyclique C dans R_n.*
1) Le code C peut être décrit par

$$C = \{p(x) \in R_n \mid p(x)h(x) \equiv 0\}$$

2) Si $h(x) = h_o + h_1x + ... + h_{n-r}x^{n-r}$, alors une matrice de contrôle de parité pour C est donnée par :

$$H = \begin{bmatrix} h_{n-r} & \cdots & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-r} & \cdots & \cdots & h_0 & 0 & \cdots & 0 \\ 0 & 0 & h_{n-r} & \cdots & \cdots & h_0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \cdots & \ddots & 0 & \\ 0 & 0 & \cdots & 0 & h_{n-r} & \cdots & \cdots & h_0 \end{bmatrix}.$$

3) Le code dual $C^\perp$ est le code cyclique du de dimension r avec polynôme générateur :

$$h^\perp(x) = h_0^{-1}x^{n-r}h(x^{-1}) = h_0^{-1}(h_0x^{n-r} + h_1x^{n-r-1} + ... + h_{n-r})$$

où le dernier polynôme entre parenthèses est le polynôme inverse du polynôme de contrôle $h(x)$. (Notez que $C^\perp$ n'est pas généré par $h(x)$).

Exemple 2.4.8 *Le code $C_1 = \langle x^6+x^3+1 \rangle$ a un polynôme de contrôle*

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

et depuis $h^\perp(x) = x^3(x^{-3}-1) = x^3+1$, le code C_1 a une matrice de contrôle

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

Codes cycliques minimaux

Parmi tous les codes cycliques en $\mathcal{R}_n$, deux types spéciaux méritent d'être mentionnés. Supposons que

$$x^n - 1 = \prod_i m_i(x)$$

est la factorisation de x^n-1 en polynômes irréductibles sur $\mathbb{F}_q$.D'après le théorème 2.2.5, les codes cycliques $M_i = \langle m_i(x) \rangle$ sont maximaux, car le seul cyclique code qui contient correctement M_i est $\mathcal{R}_n$ lui-même. De même, si nous laissons

$$\hat{m}_i(x) = \frac{x^n - 1}{m_i(x)}$$

alors les codes cycliques $\hat{M}_i = \langle \hat{m}_i(x) \rangle$ sont minimaux, puisque le seul code cyclique dans $\mathcal{R}_n$ qui est correctement contenu dans $\hat{M}_i$, est le code zéro $\{0\}$. Les codes cycliques minimaux sont également appelés **codes irréductibles.**

Exemple 2.4.9 *Nous avons vu que le polynôme* $x^7 - 1$ *sur* $\mathbb{F}_2$ *se factorise de la forme.* $x^7 - 1 = (x+1)(x^3+x^2+1)(x^3+x+1)$ *Les trois facteurs étant irréductible. Alors,*
1.les codes cyclique maximaux sont :

$$M_1 = \langle m_1(x) \rangle = \langle x+1 \rangle,$$
$$M_2 = \langle m_2(x) \rangle = \langle x^3+x^2+1 \rangle \text{ ;}$$
$$M_3 = \langle m_3(x) \rangle = \langle x^3+x+1 \rangle$$

2.les codes cyclique minimaux sont $\hat{M}_1 = \langle \hat{m}_1(x) \rangle$,$\hat{M}_2 = \langle \hat{m}_2(x) \rangle$ *et* $\hat{M}_3 = \langle \hat{m}_3(x) \rangle$ *avec les polynômes génératrices :*

$$\hat{m}_1(x) = \frac{x^7 - 1}{x+1} = (x^3+x^2+1)(x^3+x+1) = 1+x+x^2+3x^3+x^4+x^5+x^6$$

$$\hat{m}_2(x) = \frac{x^7 - 1}{x^3 + x^2 + 1} = (x+1)(x^3+x+1) = 1+2x+x^2+x^3+x^4$$

$$\hat{m}_3(x) = \frac{x^7 - 1}{x^3 + x + 1} = (x+1)(x^3+x^2+1) = 1+x+x^2+2x^3+x^4$$

Chapitre 3

Les idempotents primitifs

Dans ce chapitre, nous explorons une autre approche pour décrire les codes cycliques, impliquant un type de polynôme différent du polynôme générateur.

3.1 Le générateur idempotent d'un code cyclique

Soit $n \in \mathbb{N}^*$ et q une puissance d'un nombre premier p et $\mathbb{F}_q$ le corps finit à q éléments.

Définition 3.1.1 *Un polynôme $e(x) \in \mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$ est dit **idempotent** dans $\mathcal{R}_n$ si*

$$e^2(x) \equiv e(x) \ .$$

Exemple 3.1.1 *Le polynôme $x^3 + x^5 + x^6$ est idempotent dans $\mathcal{R}_7$, puisque*

$$(x^3 + x^5 + x^6)^2 \equiv x^3 + x^5 + x^6.$$

Théorème 3.1.1 *Soit C un code cyclique dans $\mathcal{R}_n$ ((n,q)=1), avec de polynôme générateur $g(x)$ et de polynôme de contrôle $h(x)$. Alors $g(x)$ et $h(x)$ sont premier entre eux, et donc il existe des polynômes $a(x)$ et $b(x)$ pour lesquels*

$$a(x)g(x) + b(x)h(x) = 1. \tag{3.1}$$

Le polynôme $e(x) = a(x)g(x)mod(x^n - 1)$ a les propriétés suivantes :

1. *L'idempotent $e(x)$ est l'identité unique en C, c'est-à-dire*

$$p(x)e(x) \equiv p(x) \text{ pour tout } p(x) \in C.$$

2. *L'idempotent $e(x)$ est le polynôme unique en C qui est à la fois idempotent et engendré C, c'est-à-dire $C = \langle e(x) \rangle$.*

Preuve 3.1.1 *1.Si $e_1(x)$ et $e_2(x)$ sont deux identités dans $\mathcal{R}_n$, alors*

$$e_1(x) \equiv e_1(x)e_2(x) \equiv e_2(x)$$

Donc $e_1(x) = e_2(x)$.
Ainsi, si une identité existe, elle est unique.
Puisque $g(x)h(x) = x^n - 1$ n'a pas de racines multiples dans n'importe quel extension de corp $\mathbb{F}_q$, $g(x)$ et $h(x)$ sont premier entre eux, et donc (3.1) *est vrai.*

2. Si $p(x) \in C$, alors $p(x)h(x) \equiv 0$, et ainsi (3.1) *donne*

$$a(x)g(x)p(x) \equiv p(x)$$

Alors $e(x) = a(x)g(x) mod(x^n - 1)$ est l'identité en C et aussi que $e(x)$ engendré C puisque tout polynôme en C est un multiple de $e(x)$. La multiplication (3.1) *par $a(x)g(x)$ donne*

$$[a(x)g(x)]^2 + a(x)b(x)g(x)h(x) = a(x)g(x)$$

Donc

$$[a(x)g(x)]^2 \equiv a(x)g(x)$$

Donc $e(x)$ est idempotent.

Pour compléter la preuve, il suffit de montrer qu'un idempotent $f(x)$ qui génère également C doit être égal à $e(x)$. Puisque $f(x)$ engendré C, il existe un $q(x) \in \mathcal{R}_n$, pour lequel $e(x) \equiv q(x)f(x)$. Par conséquent,

$$f(x) \equiv e(x)f(x) \equiv q(x)f^2(x) \equiv q(x)f(x) \equiv e(x)$$

ce qui implique que $f(x) = e(x)$. Ceci complète la preuve.

Exemple 3.1.2 *Soit $C = \langle 1 + x^2 + x^3 + x^4 \rangle$ un code cyclique dans $R_7 = \mathbb{F}_2[x]/(x^7 - 1)$, et considérons le polynôme $e(x) = x^3(1 + x^2 + x^3 + x^4) = 1 + x^3 + x^5 + x^6$ dans ce code.*
$e^2(x) = (1 + x^3 + x^5 + x^6)^2 = 1 + x^6 + x^3 + x^5 = e(x)$, donc $e(x)$ un idempotent.
Puisque,

$$\begin{aligned} g(x)e(x) &= (1 + x^2 + x^3 + x^4)(1 + x^3 + x^5 + x^6) \\ &= (1 + x^3 + x^5 + x^6) + (x^2 + x^5 + 1 + x) \\ &+(x^3 + x^6 + x + x^2) + (x^4 + 1 + x^2 + x^3) \\ &= 1 + x^2 + x^3 + x^4 \\ &= g(x). \end{aligned}$$

$g(x) \in \langle e(x) \rangle$ et donc $C = \langle e(x) \rangle$. Alors $e(x)$ est un générateur idempotent de C.

Théorème 3.1.2 *Chaque code cyclique C de longueur n sur le corps $\mathbb{F}_q$ ((n,q)=1) a un générateur idempotent $e(x)$.*

Preuve 3.1.2 *Soit $g(x)$ le polynôme générateur du code cyclique C. Alors*

$$x^n - 1 = g(x)h(x)$$

dans $\mathbb{F}_q[x]$. Par notre hypothèse sur n, $x^n - 1$ a n distinct facteurs de sorte que

$$gcd\,(g(x), h(x)) = 1$$

Par l'algorithme euclidien, il y a polynômes $a(x)$ et $b(x)$ de sorte que

$$a(x)g(x) + b(x)h(x) = 1$$

dans $\mathbb{F}_q[x]$. Poson $e(x) = a(x)g(x)$. Il est Clairement que $e(x)$ est dans C.
Par conséquent

$$a(x)g(x) = a^2(x)g^2(x) + a(x)b(x)g(x)h(x) = a^2(x)g^2(x)$$

à $\mathbb{R}_n$ *. Si* $c(x)$ *est un mot de code quelconque en C, alors* $c(x) = d(x)g(x)$ *de sorte que*

$$c(x) = a(x)g(x)c(x) + b(x)d(x)g(x)h(x)$$

dans $\mathbb{F}[x]$*, et ceci est égal à* $a(x)g(x)c(x)$ *dans* $\mathbb{R}_n$ *. D'où* $c(x) = e(x)c(x)$ *de sorte que* $e(x)$ *agit comme une unité pour C et ainsi génère C.*

Exemple 3.1.3 *L'idempotent générateur pour le code cyclique zéro {0} est 0, tandis que celui pour le code cyclique* $\mathcal{R}_n$ *est 1*

Théorème 3.1.3 *Si* $e(x)$ *est le générateur idempotent de C,alors le polynôme générateur* $g(x)$ *de C est égal à*

$$g(x) = gcd(e(x), (x^n - 1))$$

Preuve 3.1.3 *En référence à* (3.1)*, puisque* $x^n - 1 = g(x)h(x)$ *et* $e(x) \equiv a(x)g(x)$*, nous avons*

$$gcd(e(x), x^n - 1) = gcd(a(x)g(x), h(x)g(x))$$

Mais, selon (3.1)*,*$a(x)$ *et* $h(x)$ *sont relativement premiers, donc c'est égal à* $g(x)$*.*

Exemple 3.1.4 *Le tableau suivant donne tous les codes cycliques* C_i *de longueur 7 sur* $\mathbb{F}_2$ *ainsi que leurs polynômes générateurs* $g_i(x)$ *et leurs idempotents générateurs* $e_i(x)$ *;*

i	dim	$g_i(x)$	$e_i(x)$
0	*0*	$1+x^7$	*0*
1	*1*	$1+x+x^2+...+x^6$	$1+x+x^2+...+x^6$
2	*3*	$1+x^2+x^3+x^4$	$1+x^3+x^5+x^6$
3	*3*	$1+x+x^2+x^4$	$1+x+x^2+x^4$
4	*4*	$1+x+x^3$	$x+x^2+x^4$
5	*4*	$1+x^2+x^3$	$x^3+x^5+x^6$
6	*6*	$1+x$	$x+x^2+...+x^6$
7	*7*	*1*	*1*

Théorème 3.1.4 *Soit C un $[n,k]$-code cyclique de polynôme idempotent $e(x)=\sum_{n-1}^{i=0} e_i x^i$.Alors la matrice :*

$$\begin{pmatrix} e_0 & e_1 & e_2 & \dots & e_{n-2} & e_{n-1} \\ e_{n-1} & e_0 & e_1 & \dots & e_{n-3} & e_{n-2} \\ & & & \dots & & \\ e_{n-k+1} & e_{n-k+2} & e_{n-k+3} & \dots & e_{n-k-1} & e_{n-k} \end{pmatrix}$$

est une matrice génératrice de C.

Preuve 3.1.4 *Cela revient à dire que $\{e(x), xe(x), ..., x^{k-1}e(x)\}$ est une base de C. Par conséquent il suffit de montrer que si $a(x) \in \mathbb{F}_q[x]$ a un degré inférieur à k tel que $a(x)e(x)=0$, alors $a(x)=0$. Soit $g(x)$ le polynôme générateur pour C. Si $a(x)e(x)=0$, alors $0=a(x)e(x)g(x)=a(x)g(x)$ car $e(x)$ est l'unité de C par le théorème (1), sauf si $a(x)=0$.*

Si C_1 et C_2 sont des codes de longueur n sur $\mathbb{F}_q$, alors $C_1+C_2=\{c_1+c_2 \mid c_1 \in C_1 \text{ et } c_2 \in C_2\}$ est la somme de C_1 et C_2. L'intersection et la somme de deux codes cycliques sont cycliques, et leurs polynômes générateurs et générateurs d'idempotents sont déterminés dans le prochain théorème.

Théorème 3.1.5 *Soit C_i un code cyclique de longueur n sur $\mathbb{F}_q$ et idempotent générateur $e_i(x)$ pour $i=1$ et 2. Alors :*

1. *$C_1 \subset C_2$ si et seulement si $e_1(x)e_2(x) \equiv e_1(x)$,*
2. *$C_1 \cap C_2$ a polynôme générateur $lcm(g_1(x), g_2(x))$ et idempotent générateur $e_1(x)e_2(x)$.*
3. *$C_1 + C_2$ a un générateur polynomial $gcd(g_1(x), g_2(x))$ et idempotent générateur. $e_1(x) + e_2(x) - e_1(x)e_2(x)$.*

Preuve 3.1.5 *On montre que la somme de deux codes cycliques est cyclique.*
Soit $g(x) = pgcd(g_1(x), g_2(x))$. Ça suit de l'algorithme euclidien que

$$g(x) = g_1(x)a(x) + g_2(x)b(x)$$

pour certains $a(x)$ et $b(x)$ en $\mathbb{F}_q[x]$. Donc $g(x) \in C_1 + C_2$. Puisque $C_1 + C_2$ est cyclique, $\langle g(x) \rangle \subseteq C_1 + C_2$. D'autre part $g(x)|g_1(x)$, qui montre que $C_1 \subseteq \langle g(x) \rangle$, de même $C_2 \subseteq \langle g(x) \rangle$ impliquant $C_1 + C_2 \subseteq \langle g(x) \rangle$. Donc $C_1 + C_2 = \langle g(x) \rangle$. Puisque $g(x)|(x^n - 1)$ en $g(x)|g_1(x)$ et $g(x)$ est unique, Alors $g(x)$ est le polynôme générateur pour $C_1 + C_2$.

Si $c(x) = c_1(x) + c_2(x)$ où $c_i(x) \in C_i$ pour $i = 1$ et 2, puis

$$\begin{aligned} & c(x)(e_1(x) + e_2(x) - e_1(x)e_2(x)) \\ &= c_1(x) + c_1(x)e_2(x) - c_1(x)e_2(x) \\ &+ c_2(x)e_1(x) + c_2(x) - c_2(x)e_1(x) \\ &= c(x) \ . \end{aligned}$$

De sort que $e_1(x) + e_2(x) - e_1(x)e_2(x)$ agit comme une unité pour $C_1 + C_2$ et la génère aussi

Exemple 3.1.5 *$C_1 = \langle g_1 \rangle$ et $C_2 = \langle g_2 \rangle$ deux codes cycliques sur $\mathbb{F}_2$ avec , $g_1(x) = (1 + x)(1 + x + x^3)$ et $g_2(x) = (1 + x)(1 + x + x^3)$ et leurs idempotents générateurs $e_1(x) = 1 + x^3 + x^5 + x^6$, $e_2(x) = 1 + x + x^2 + x^4$.*
Et soient $c_1 \in C_1$ et $c_2 \in C_2$ avec $c_1 = (x+x^2+x^4)$ et $c_2 = (x+x^3+x^4)$
1. Le code cyclique $C_1 + C_2$ a un polynôme générateur $g(x)$ avec

$$\begin{aligned} g(x) &= \gcd(g_1(x), g_2(x)) \\ &= \gcd((1+x)(1+x+x^3), (1+x)(1+x+x^3)) \\ &= (1+x) \end{aligned}$$

On a

$$c_1 + c_2 = (x^2 + x^3) = x^2(1+x) = x^2 g(x) \in (C_1 + C_2)$$

2. Soit $e_1 + e_2 - e_1e_2 = x(1+x)(1+x^2+x^4)$ *on a*

$$(x(1+x)(1+x^2+x^4))^2 = x(1+x)(1+x^2+x^4)$$

Donc, $e_1 + e_2 - e_1e_2$ *est un générateur idempotent de* $C_1 + C_2$

D'autre part, $(c_1+c_2)(e_1+e_2-e_1e_2) = (x^2+x^3)x(1+x)(1+x^2+x^4) = x^2+x^3 = (c_1+c_2)$.

Théorème 3.1.6 *Soit* C *un code cyclique dans* $\mathcal{R}_n$ *de le polynôme générateur* $g(x)$ *et idempotent générateur* $e(x)$. *Alors* $g(x)$ *et* $e(x)$ *ont exactement les mêmes racines, dans le corps de décomposition pour* $x^n - 1$, *parmi les n-ième racines de l'unité.*

De plus, si $f(x)$ *est un idempotent dans* $\mathcal{R}_n$, *qui a exactement les mêmes racines que* $g(x)$ *parmi les n-ième racines de l'unité, alors* $f(x)$ *est l'idempotent générateur de* $\langle g(x) \rangle$.

Preuve 3.1.6 *Soit* α *une nième racine primitive d'unité. Puisque* $e(x) = a(x)g(x)$, *on en déduit que* $g(\alpha^i) = 0$ *implique* $e(\alpha^i) = 0$. *Par contre, si h(x) est le polynôme de contrôle pour C, alors* $g(\alpha^i) = 0$ *si et seulement si* $h(\alpha^i) \neq 0$. *Par conséquent, par (1),* $e(^i) = 0$ *implique* $h(\alpha^i) \neq 0$, *ce qui implique que* $g(\alpha^i) = 0$.

Pour la deuxième partie du théorème, nous observons que puisque chaque racine de $g(x)$ *est une racine de* $f(x)$, *et puisque* $g(x)$ *n'a pas de racines multiples dans n'importe quelle extension, nous devons avoir* $g(x) \mid f(x)$. *De plus, comme les racines du polynôme de contrôle* $h(x)$ *sont précisément les non-racines de* $g(x)$, *parmi les n-èmes racines de l'unité, nous voyons que* $h(x)$ *et* $f(x)$ *n'ont pas de*

racines communes dans n'importe quelle extension. Par conséquent, ils sont relativement premiers. Mais si D est le code cyclique dans $\mathcal{R}_n$. avec génération idempotente $f(x)$, alors par le théorème 3, le polynôme générateur pour D est

$$gcd\,(f(x), x^n - 1) = gcd\,(f(x), h(x)g(x)) = g(x)$$

et donc $D = C$. Ainsi, $f(x)$ est l'idempotent générateur de C.

Théorème 3.1.7 *Soit $C = \langle e(x) \rangle$ un code cyclique avec polynôme de contrôle h(x). puis le code cyclique $\langle h(x) \rangle$ a un idempotente générateur $1 - e(x)$ et le code dual de C, $C^{\perp} = \langle h^{\perp}(x) \rangle$ a un idempotent générateur*

$$[1 - e(x^{n-1})] \bmod (x^n - 1)$$

Preuve 3.1.7 *puisque*

$$h(x)(1 - e(x)) \equiv h(x)(1 - a(x)g(x)) \equiv h(x)$$

on voit que $1 - e(x)$ est l'identité dans $\langle h(x) \rangle$. De même,puisque $h^{\perp}(x) = h_0^{-1} x^k h(x^{-1}) \equiv h_0^{-1} x^k h(x^{n-1})$, nous avons

$$\begin{aligned} h^{\perp}(x)(1 - e(x^{n-1})) &\equiv h^{\perp}(x) - h_0^{-1} x^k h(x^{n-1}) e(x^{n-1}) \\ &\equiv h^{\perp}(x) - h_0^{-1} x^k h(x^{n-1}) a(x^{n-1}) g(x^{n-1}) \\ &\equiv h^{\perp}(x) \end{aligned}$$

et donc $[1 - e(x^{n-1})] \bmod (x^n - 1)$ est l'identité dans $C^{\perp} = \langle h^{\perp}(x) \rangle$.

Exemple 3.1.6 *Le tableau suivant donne tous les codes cycliques C_i de longueur 7 sur $\mathbb{F}_2$ ainsi que leurs idempotents générateurs $e_i(x)$ et les idempotents générateurs de leurs codes duaux.*

i	dim	$e_i(x)$	$[1 - e_i(x^{n-1})] \bmod (x^n - 1)$
0	*0*	*0*	*1*
1	*1*	$1 + x + x^2 + ... + x^6$	$x + x^2 + ... + x^6$
2	*3*	$1 + x^3 + x^5 + x^6$	$x^3 + x^5 + x^6$
3	*3*	$1 + x + x^2 + x^4$	$x + x^2 + x^4$
4	*4*	$x + x^2 + x^4$	$1 + x + x^2 + x^4$
5	*4*	$x^3 + x^5 + x^6$	$1 + x^3 + x^5 + x^6$
6	*6*	$x + x^2 + ... + x^6$	$1 + x + x^2 + ... + x^6$
7	*7*	*1*	*0*

3.2 Les idempotents primitifs dans $\mathcal{R}_n = \mathbb{F}_q[x]/(x^n - 1)$

Définition 3.2.1 *L'idempotent générateur d'un code cyclique minimal $\hat{M}_i = \langle \hat{m}_i(x) \rangle$ est appelé* ***idempotent primitif*** *et est noté $\theta_i(x)$.*

Théorème 3.2.1 *Soit $\theta_1(x), ..., \theta_s(x)$ des idempotents primitifs dans $\mathcal{R}_n$, Alors*

1. *$\theta_i(x)\theta_j(x) \equiv 0$ pour $i \neq j$,*

2. *$\theta_i(x) + ... + \theta_i(x) = 1$,*

3. *L'idempotent générateur du code $\langle m_{i_1} m_{i_2} ... m_{i_k} \rangle$ est*

$$1 - \theta_{i_1}(x) - \theta_{i_2}(x) - ... - \theta_{i_k}(x).$$

Preuve 3.2.1 *1. D'après le théorème 3.1.5 $\theta_i(x)\theta_j(x) \mod (x^n - 1)$ est l'identité du code $\hat{M}_i \cap \hat{M}_j$. Mais puisque $\hat{M}_i$ et $\hat{M}_j$ sont minimaux, leur intersection n'est constituée que du polynôme zéro.*

2. En utilisant le théorème 3.1.5 et la partie 1), nous déduisons que

$$\hat{M}_1 + \hat{M}_2 + ... + \hat{M}_s = [\theta_1(x) + ... + \theta_s(x)]$$

Mais $\hat{M}_1 + \hat{M}_2 + ... + \hat{M}_s = \mathcal{R}_n$ *qui a l'élément d'identité 1.*

3. Soit

$$\hat{m}_{j_1 j_2 ... j_r}(x) = \frac{x^n - 1}{m_{j_1}(x) m_{j_2}(x) ... m_{j_r}(x)}$$

Alors puisque

$$\hat{m}_{j_1 j_2 ... j_r}(x) = pgcd(\hat{m}_{j_1}(x) \hat{m}_{j_2}(x) ... \hat{m}_{j_r}(x))$$

nous déduisons que

$$\langle \hat{m}_{j_1 j_2 ... j_r}(x) \rangle = \hat{M}_{j_1} + \hat{M}_{j_2} + ... + \hat{M}_{j_r} = [\theta_{j_1}(x) + \theta_{j_2}(x) + ... + \theta_{j_r}]$$

Si $\{i_1, ..., i_k\} = \{1, ..., s\} - \{j_1, ...j_r\}$*, puis la partie 2 donne*
$\langle m_{i_1}(x) m_{i_2}(x) ... m_{i_k}(x) \rangle = [1 - \theta_{i_1}(x) - \theta_{i_2}(x) - ... - \theta_{i_k}(x)]$.

Passons maintenant à la question de savoir comment trouver des idempotents sans prendre en compte $x^n - 1$*. Nous limitons l'attention dans cette sous-section au cas* $q = 2$*.*
Dans $\mathbb{F}_2$*, nous avons* $f^2(x) = f(x^2)$*, et donc un polynôme* $e(x) = e_o + e_1 x + ... + e_{n-1} x^{n-1}$ *dans* $\mathcal{R}_n$*, est idempotent si et seulement si*

$$e(x^2) \equiv e(x)$$

Dans $\mathcal{R}_n$ *,cela vaut si et seulement si à chaque fois* $e_i \neq 0$*, alors* $e_{2i(mod n)} \neq 0$*. Il s'ensuite que* $e(x)$ *doit être une somme de polynômes de la forme*

$$x^i + x^{2i} + ... + x^{2^{d-1} i}$$

où les exposants forment une classe cyclotomique. Nous avons établi ce qui suit.

Théorème 3.2.2 *Soit* $q = 2$*, Les idempotents dans* $\mathcal{R}_n$ *sont précisément les sommes des polynômes de la forme*

$$x^i + x^{2i} + ... + x^{2^{d-1} i}$$

où $C_i = \{i, 2i, ..., 2^{d-1}i\}$ *est un sous-ensemble cyclotomique pour 2 modulo n.*

Exemple 3.2.1 *Soit* $n = 9$*, les classes cyclotomiques pour* 2 *modulo* 9 *sont*

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\}, C_3 = \{3, 6\}.$$

donc il y a $2^3 = 8$ *idempotents :*

$$\begin{aligned}
e_1(x) &= 0 \\
e_2(x) &= x^0 = 1 \\
e_3(x) &= x + x^2 + x^4 + x^5 + x^7 + x^8 \\
e_4(x) &= x^3 + x^6 \\
e_5(x) &= e_2(x) + e_3(x) \\
e_6(x) &= e_2(x) + e_4(x) \\
e_7(x) &= e_3(x) + e_4(x) \\
e_8(x) &= e_2(x) + e_3(x) + e_4(x)
\end{aligned}$$

Les polynômes générateurs correspondant peuvent être calculés en utilisant le théorème 3.1.3. Par exemple, l'Algorithme Euclidien donne

$$g_3(x) = gcd(e_3(x), x^9 - 1) = x - 1$$

Exemple 3.2.2 *Soit* $n = 7$*, les classes cyclotomiques pour* 2 *modulo* 7 *sont :*

$$C_0 = \{0\}, C_1 = \{1, 2, 4\}, C_3 = \{3, 5, 6\}$$

donc il y a $2^3 = 8$ *idempotents*

$$\begin{aligned}
e_1(x) &= 0 \\
e_2(x) &= x^0 = 1 \\
e_3(x) &= x + x^2 + x^4 \\
e_4(x) &= x^3 + x^5 + x^6 \\
e_5(x) &= e_2(x) + e_3(x) \\
e_6(x) &= e_2(x) + e_4(x) \\
e_7(x) &= e_3(x) + e_4(x) \\
e_8(x) &= e_2(x) + e_3(x) + e_4(x)
\end{aligned}$$

Les polynômes générateurs correspondant peuvent être calculés en utilisant le théorème 3.1.3, Par exemple, l'Algorithme Euclidien donne

$$g_3(x) = gcd(e_3(x), x^7 - 1) = 1 + x + x^3$$

3.3 Une formule pour les idempotents primitifs

Lorsque nous avons accès aux n-ièmes racines de l'unité sur $\mathbb{F}_q$, nous pouvons obtenir une formule explicite pour les idempotents primitifs. Considérons la factorisation :

$$x^n - 1 = \prod_i m_i(x)$$

de $x^n - 1$ en facteurs irréductibles sur $\mathbb{F}_q$,où

$$m_i(x) = \prod_{j \in C_i} (x - \alpha^j)$$

et $C_i = \{i, qi, ..., q^{d-1_i}\}$. Nous avons besoin de quelques lemmes préliminaires ,

Lemme 3.3.1 *Soit α une racine n-ième primitive de l'unité sur $\mathbb{F}_q$. Alors pour $i = 0, ..., n-1$,*

$$\sum_{j=0}^{n-1} (\alpha^i)^j = n\delta_{i,0}$$

Preuve 3.3.1 *Si $i = 0$, le résultat est clair. Si $i \geq 0$, alors $\alpha^j \neq 1$, et donc*

$$\sum_{j=0}^{n-1} (\alpha^i)^j = \frac{1-(\alpha^i)^n}{1-\alpha^i} = 0$$

Le lemme suivant montre comment récupérer un polynôme de degré $n-1$ ou moins à partir de ses valeurs sur les racines n-èmes de l'unité.

Lemme 3.3.2 *Soit $P(x) = p_o + p_1 x + ... + p_{p-1} x^{n-1}$ un polynôme sur $\mathbb{F}_q$ et soit α une racine n-ième primitive de l'unité sur $\mathbb{F}_q$. Alors*

$$p_i = \frac{1}{n} \sum_{j=0}^{n-1} p(\alpha^j) \alpha^{-ij}$$

.

Preuve 3.3.2 *Nous avons*

$$\begin{aligned}\frac{1}{n}\sum_{j=0}^{n-1} p(\alpha^j)\alpha^{-ij} &= \frac{1}{n}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} p_k\alpha^{jk}\alpha^{-ij} \\ &= \frac{1}{n}\sum_{k=0}^{n-1} p_k \sum_{j=0}^{n-1}\alpha^{j(k-i)} \\ &= \frac{1}{n}\sum_{k=0}^{n-1} p_k n\delta_{k,j} = p_i\end{aligned}$$

Supposons maintenant que $\theta_k(x) \in \mathbb{F}_q[x]$ *est l'idempotent primitif pour le code minimal* $\hat{M}_k = \langle \hat{m}_k(x)\rangle$ *dans* $\mathcal{R}_n$. *Puisque* $\theta_k(x)$ *est idempotent, nous avons* $\theta_k^2(x) \equiv \theta_k(x) \mod (x^n - 1)$, *et donc*

$$\theta_k^2(x) = \theta_k(x) + f(x)(x^n - 1)$$

pour certain polynôme $f(x)$. *Par conséquent,*

$$\theta_k^2(\alpha^j) = \theta_k(\alpha^j)$$

et ainsi $\theta_k(\alpha^j) = 0$ *ou 1. Mais le théorème 3.1.6 dit que* $\theta_k(x)$ *et* $\hat{m}_k(x)$ *ont les mêmes zéros parmi les n-ième racines de l'unité, et donc*

$$\theta_k(\alpha^j) = \begin{cases} 0 & if \quad j \notin C_k \\ 1 & if \quad j \in C_k \end{cases}$$

Si $\theta_k(x) = \sum_{i=0}^{n-1} e_i x^i$. *Nous pouvons appliquer le lemme 3.3.2 pour obtenir*

$$e_i = \frac{1}{n}\sum_{j=0}^{n-1}\theta_k(\alpha^j)\alpha^{-ij} = \frac{1}{n}\sum_{j\in C_k}\alpha^{-ij}$$

Cela prouve ce qui suit.

Théorème 3.3.1 *Soit* $\hat{M}_k = \langle \hat{m}_k(x)\rangle$ *un code cyclique minimal dans* $\mathcal{R}_n$ *et supposons que*

$$m_k(x) = \prod_{j \in C_k} (x - \alpha^j)$$

Où C_k est un classe cyclotomique. Alors l'idempotent primitif pour $\hat{M}_k$, est

$$\theta_k(x) = \frac{1}{n} \sum_{i=0}^{n-1} \left(\sum_{j \in C_k} \alpha^{-ij} \right) x^i$$

Tous les calcules sont fait dans le corps de décomposition de $x^n - 1$ sur $\mathbb{F}_q$.

Exemple 3.3.1 *Soit α la racine $7^{-i\text{ème}}$ primitive de l'unité sur $\mathbb{F}_2$. Puisque les classes cyclotomiques de 2 modulo 9 sont :*

$$C_o = \{0\}, C_1 = \{1, 2, 4\}, C_3 = \{3, 5, 6\}$$

nous avons

$$\theta_0(x) = 1 + x + ... + x^6$$

$$\theta_1(x) = \Sigma_{i=0}^{6} (\alpha^{-i} + \alpha^{-2i} + \alpha^{-4i}) x^i$$

$$\theta_3(x) = \Sigma_{i=0}^{6} (\alpha^{-3i} + \alpha^{-6i} + \alpha^{-5i}) x^i$$

Le corps de décomposition de $x^7 - 1$ sur $\mathbb{F}_2$, est $\mathbb{F}_{q^s}$, où $s = ord_7(2) = 3$,
Les calcules des coefficients de $\theta_1(x)$ et $\theta_3(x)$ sont fait dans $\mathbb{F}_{2^3}$. puisque $8 = 2^3$, nous considérons un polynôme binaire de degré 3 irréductible, par exemple $f(x) = x^3 + x + 1$.on a :

$$f(\alpha) = 0 \Longrightarrow \alpha^3 + \alpha + 1 = 0 \Longrightarrow \alpha^3 = \alpha + 1$$

on a donc :

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

nous calculons maintenant les coefficients de $\theta_1(x)$

coef de x^0 : $1 + 1 + 1 = 1$

coef de $x^1 : \alpha^{-1} + \alpha^{-2} + \alpha^{-4} = \alpha^6 + \alpha^5 + \alpha^3 = +\alpha^2 + 1 + \alpha^2 + \alpha + 1 + \alpha + 1 = 1$

coef de $x^2 : \alpha^{-2} + \alpha^{-4} + \alpha^{-8} = \alpha^5 + \alpha^3 + \alpha^6 = 1$

coef de $x^3 : \alpha^{-3} + \alpha^{-6} + \alpha^{-12} = \alpha^4 + \alpha + \alpha^2 = \alpha^2 + \alpha + \alpha + \alpha^2 = 0$

coef de $x^4 : \alpha^{-4} + \alpha^{-8} + \alpha^{-16} = \alpha^3 + \alpha^6 + \alpha^5 = 1$

coef de $x^5 : \alpha^{-5} + \alpha^{-10} + \alpha^{-20} = \alpha^2 + \alpha^4 + \alpha = 0$

coef de $x^6 : \alpha^{-6} + \alpha^{-12} + \alpha^{-24} = \alpha + \alpha^2 + \alpha^4 = 0$

Donc,

$$\theta_1(x) = 1 + x + x^2 + x^4$$

Et

$$\theta_3(x) = \sum_{i=0}^{6} (\alpha^{-3i} + \alpha^{-6i} + \alpha^{-5i}) x^i$$

$$= 1 + (\alpha^{-3} + \alpha^{-6} + \alpha^{-5})x + (\alpha^{-6} + \alpha^{-12} + \alpha^{-10})x^2$$

$$+ (\alpha^{-9} + \alpha^{-18} + \alpha^{-15})x^3 + (\alpha^{-12} + \alpha^{-24} + \alpha^{-20})x^4$$

$$+ (\alpha^{-15} + \alpha^{-30} + \alpha^{-25})x^5 + (\alpha^{-18} + \alpha^{-36} + \alpha^{-30})x^6$$

$$= 1 + x^3 + x^5 + x^6$$

Exemple 3.3.2 *Soit* α *une 9ème racine primitive de unité sur* $\mathbb{F}_2$. *Puisque les classes cyclotomiques pour* 2 *modulo* 9 *sont :*

$$C_o = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\}, C_3 = \{3, 6\}$$

nous avons

$$\theta_0(x) = 1 + x + ... + x^8$$

$$\theta_1(x) = \sum_{i=0}^{8} (\alpha^{-i} + \alpha^{-2i} + \alpha^{-4i} + \alpha^{-5i} + \alpha^{-7i} + \alpha^{-8i}) x^i$$

$$\theta_3(x) = \sum_{i=0}^{8} (\alpha^{-3i} + \alpha^{-6i}) x^i$$

Calculons $\theta_3(x)$. *Le corps de décomposition pour* $x^9 - 1$ *sur* $\mathbb{F}_2$, *est* $\mathbb{F}_{q^s}$, *où* $s = ord_9(2) = 6$, *c'est-à-dire* $\mathbb{F}_{64}$ *De plus, si* β *est un élément*

primitif de $\mathbb{F}_{64}$*, alors* $\alpha = \beta^7$ *est une n-ième racine primitive d'unité. En se référant à la table des corps pour* $\mathbb{F}_{64}$ *en annexe, nous voyons que les coefficients de* $\theta_3(x)$ *sont :*

coef de $x^0 : 1 + 1 = 0$
coef de $x^1 : \alpha^{-3} + \alpha^{-6} = \alpha^3 + \alpha^6 = \beta^{42} + \beta^{21} = 111010 + 111011 = 1$
coef de $x^2 : \alpha^{-6} + \alpha^{-12} = \alpha^3 + \alpha^6 = 1$
coef de $x^3 : \alpha^{-9} + \alpha^{-18} = 1 + 1 = 0$
coef de $x^4 : \alpha^{-12} + \alpha^{-24} = \alpha^8 + \alpha^3 = 1$
coef de $x^5 : \alpha^{-15} + \alpha^{-30} = \alpha^3 + \alpha^6 = 1$
coef de $x^6 : \alpha^{-18} + \alpha^{-36} = \alpha^{-3} = 1 + 1 = 0$
coef de $x^7 : \alpha^{-21} + \alpha^{-42} = \alpha^3 + \alpha^3 = 1$
coef de $x^8 : \alpha^{-24} + \alpha^{-48} = \alpha^3 + \alpha^6 = 1$

Alors,

$$\theta_3(x) = x + x^2 + x^4 + x^5 + x^7 + x^8$$

qui est l'idempotent $e_3(x)$ *dans l'exemple 3.2.1*

Exemple 3.3.3 • *Les codes cycliques irréductibles (minimaux) de longueur* 7 *sur* $\mathbb{F}_2$

Code	*Dim*	*I.P*	*Polynôme générateur*
C_0	*1*	$1 + x + ... + x^6$	$1 + x + ... + x^6$
C_1	*3*	$1 + x + x^2 + x^4$	$1 + x + x^2 + x^4$
C_2	*3*	$1 + x^3 + x^5 + x^6$	$x^4 + x^3 + x^2 + 1$

• *Les codes duaux des codes cycliques irréductibles de longueur* 7 *sur* $\mathbb{F}_2$

Code	*Dim*	*I.P*	*Polynôme générateur*
$C_0^\perp$	*6*	$x + x^2 + ... + x^6$	$1 + x$
$C_1^\perp$	*4*	$x + x^2 + x^4$	$1 + x + x^3$
$C_2^\perp$	*4*	$x^3 + x^5 + x^6$	$x^3 + x^2 + 1$

Conclusion

Dans ce travail nous avons présenté une cas particulier des générateurs des codes cycliques irréductibles (minimaux) qui s'appelle les idempotents primitifs.

Nous avons montré que les idempotents primitifs peuvent être générés directement ces codes à partir des classes cyclotomiques.

Bibliographie

[1] **A.A.Pantchichkine**, Magistère de Mathématique (L'ENS de Lyon) 2005.

[2] **A.Bojilov, A.J.van Zanten et S.M. Dodunekov**,Idempotent Generators of Generalized Residue Codes, Technical report, TICC, Tilburg University, 2010. To be published.

[3] **Boyer Pascal**, De l'arithmétique à la théorie des nombres. Université Sorbonne Paris Nord.

[4] **C.Blanchet**, Extensions des corps : généralités,Institut de Mathématiques de Jussieu - Paris Rive Gauche (UMR 7586).

[5] Corps finis en master S1,(Un article sur Internet).

[6] **D.J.Mercier**, Corps finis,IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre cedex 97159, dany-jack.mercier. 2003.

[7] **E.M.Souidi**, Théorie des codes correcteurs d'erreurs.2011.

[8] **E.Wegrzynowski**, Licence et Master mention informatique, USTL, 2008.

[9] **J.F.Havet**, ALGEBRE : Groupes et Applications, Université d'Orléans,2003.

[10] **K.Lutful, M. Shorfuzzaman et J. Begum**, Idempotent Polynomials : An Easy Supplant to Generator Polynomials, Université de Manitoba.Canada.2004.

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

[12] **R.Howlett**, An undergraduate course in Abstract Algebra,Université of Sydney.

[13] **S.Roman**,Coding and information theory.Springer-Verlag,1992.

[14] **S.L. Chaopingxing**,Coding Theory,A First Course,Cambridge University Press 2004.

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

[16] **V.Pless**,Introduction to the Theory of Error-Correcting Codes, Wiley-Intersci. Ser. Discrete Math. Optim. (1998).

[17] **W.C Huffman et V.Pless**, Fundamentals of Error-Correcting Codes, Combridge University Press (2003).

ملخص

الشفرة الدورية التي طولها n علي الحقل المنتهي $\mathbb{F}_q$ هي مثالي رئيسي في حلقة حاصل القسمة $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ حيث $\mathbb{F}_q[x]$هو حلقة كثيرات الحدود التي معاملاتها من $\mathbb{F}_q$ و $\langle x^n - 1\rangle$ هو المثالي الرئيسي المولد بكثير الحدود $(x^n - 1)$

في هذا البحث نهتم بالمثاليات الرئيسية لحلقة حاصل القسمة R_n التي تم إنشاؤها بواسطة البدائيين عديمي النمو.

Résumé

Un code cyclique de longueur n sur le corps fini $\mathbb{F}_q$ est un idéal principal de l'anneau quotient $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ où $\mathbb{F}_q[x]$ est l'anneau des polynômes à coefficients dans le corps fini $\mathbb{F}_q$ et $\langle x^n - 1\rangle$ est l'idéal principal engendré par le polynôme $(x^n - 1)$.

Dans ce projet on s'intéresse aux idéaux de l'anneau quotient R_n engendré par les idempotents primitifs.

Abstract

A cyclic code of length n on the finite field $\mathbb{F}_q$ is a principal ideal of the quotient ring $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ where $\mathbb{F}_q[x]$ is the ring of polynomials with coefficients in the finite field $\mathbb{F}_q$ and $\langle x^n - 1\rangle$ is the principal ideal generated by the polynomial $(x^n - 1)$.

In this project we are interested in the ideals of the quotient ring R_n generated by the primitive idempotents.