UNIVERSITE MOHAMED BOUDIAFDE 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 : Mathématiques discrètes

Par

SELMANE Djamel

Sujet

Codes cycliques optimaux [n,n/2] sur GF(7)

Devant le jury :

Mr. A. Amroune	Prof.	Univ de M'sila	Président
Mr. C. Mihoubi	MC/B.	Univ de M'sila	Rapporteur
Mr. N. Ghadbane	MA/A.	Univ de M'sila	Examinateur

Promotion : 2015 / 2016

Remerciements

En premier lieu je remercie **ALLAH** pour m'avoir guidé et donner la force pour la finalisation de ce mémoire.

Je tiens à exprimer ma profonde gratitude à Monsieur **C.MIHOUBI**, Maître de Conférences à universite de M'sila, pour m'avoir proposé ce sujet, pour sa disponibilité et pour m'avoir suivi et guidé tout au long de ce travail.

Je remercie Monsieur **A.AMROUNE**, professeur à universite de M'sila, pour l'honneur qu'il me fait de présidé le jury de ce Mémoire.

Je remercie également Monsieur **N.GHADBANE,** Maître Assistant à universite de M'sila, pour avoir voulu faire partie du jury.

Je ne saurais oublier de remercier tous mes professeurs et toutes les personnes ayant contribué de près ou de loin à l'aboutissement de ce travail.

Pour finir mes derniers mots de remerciements vont tout naturellement à ma famille et mes amis.

Notations

- $\mid G \mid$: L'ordre d'un groupe fini ou le cardinal d'un ensemble fini G.
- $\mathbb{Z}/p\mathbb{Z}$: L'ensemble des entiers modulo p.
- $\mathbb{F}_q$: Un corps fini de cardinal q.
- $(f(X))$: L'idéal engendré par $f(X)$ dans A[X].
- $a \mid b$: a divise b.
- $C[n,k]$: Code correcteur de longueur n et dimension k.
- $\cong$: Isomorphisme de groupe, de corps, d'espaces vectoriels.
- $wt(x)$: Le poids de Hamming d'un mots x.
- $d(x,y)$: Distance de Hamming entre x et y.
- $C^{\perp}$: Le code dual du code considéré.
- $\mathbb{F}_q[X]/(f)$: Anneau des classes modulo $f(X)$.
- $\mathbb{F}_q[X]/(X^n-1)$: Anneau quotient (des classes des polynômes de degré inferieur à n).
- G : Matrice génératrice de C.
- H : Matrice de controle de C.
- ${}^tG$: Transposée d'une matrice G.

Résumé

Dans ce travail on considère les codes cycliques optimaux de rendement 1/2 sur le corps fini GF(7). Le problème central dans la théorie du codage est trouver la meilleure distance minimum d_q pour laquelle un code de paramètres [n, k,d] sur $\mathbb{F}_q$ existe. Dans ce contexte nous avons réussi à optimiser cette distance pour les codes cycliques de taux 1/2 sur GF(7) pour n pair non multiple de 7 et inferieur ou égale à 50.

Mots clés : Corps fini, anneau de polynômes , polynôme irréductible, code linéaire, distance minimale, poids de Hamming, code cyclique, polynôme générateur.

Abstract

In this work we consider the cyclic codes of rate 1/2 over the finite fields GF(7). The so-called fundamental problem in coding theory is finding the largest value of d for which a code of parameters [n, k, d] over $\mathbb{F}_q$ exists. In this context we have successfully optimize this distance for the cyclic codes of rate 1/2 over GF(7) for not even multiple n of 7 and less than or equal to 50.

Key words : Finite fields, ring polynomials, irreducible polynomial, linear code, minimum distance, Hamming weight, cyclic codes,generator polynomial .

Table des matières

Introduction

La transmission d'informations dans l'air (informations à envoyer à un satellite) ou par des câbles (lecture d'un CD) est souvent sujette à des perturbations (chocs du disc man).

C'est pour ce la qu'il convient d'introduire les codes détecteurs et correcteurs d'erreurs. C'es t-à-dire que l'on va coder les informations à envoyer de manière judicieuse afin de pouvoir justement détecter et corriger d'éventuels problèmes sous réserve qu'ils ne soient pas trop nombreux. En fait, le technicien connaît à l'avance la qualité de la transmission et aura effectue des tests statistiques pour prévoir le nombre (mais pas la position) des erreurs.

Les codes cycliques représentent la famille des codes la plus importante. D'un point de vue pratique, ce sont les codes les plus utilisés car leur mise en œuvre est facile et ils admettent de bons algorithmes de décodage. D'un point de vue théorique, ils possèdent une structure algébrique intéressante se fondent sur la théorie des corps finis, et en particulier les extensions de **Galois** ainsi que les polynômes. Les codes cycliques les plus connus sont les codes de **Hamming, BCH, Reed-Solomon**, etc.

L'objectif principal de ce mémoire est l'optimisation de la distance minimale des codes cycliques de paramètre [n,n/2], pour n pair et non multiple de 7, sur le corps fini $\mathbb{F}_7$.

Ce travail est composé de trois chapitres structurés comme suit :

- Dans le premier chapitre on donne quelques notions de base d'algèbre, ensuite on présente les notions fondamentales de la théorie des corps finis (Anneau, corps fini, les extensions des corps finis, la construction d'un corps fini).

- Dans le deuxième chapitre on présente les polynômes définie sur un corps fini et les opérations sur les polynômes, les polynômes irréductibles et la factorisation du polynôme $(X^n - 1)$ en facteurs irréductibles sur un corps fini.

- Le troisième chapitre on présente quelques des rappels de théorie de codage algébrique et on particulier les codes linéaires et les codes cycliques sur un corps fini et nous considérons les codes cycliques optimaux de rendement $1/2$ sur le corps fini $\mathbb{F}_7$, et en utilisant l'algorithme de Chen pour calculer la distance minimale pour n pair non multiple de 7 et inférieur ou égale à 50.

Chapitre 1

Etude des corps finis

Dans ce chapitre on rappelle les notions de base dont on aura besoin par la suite:

Anneau et corps, corps finis, caractéristique et cardinal d'un corps fini, groupe multiplicatif et sous corps d'un corps fini et la construction de corps fini.

1.1 Corps finis

1.1.1 Anneau et corps

Définition 1.1.1 ***(Anneau)***

Un anneau est la donnée d'un ensemble non vide A et de deux lois de composition interne, notées " $+$ " et " $\cdot$ " (appelées respectivement addition et multiplication), telles que :

(i)-$(A,+)$ est un groupe abélien (On notera 0 son élément neutre et appelé zéro de A),

(ii)- $\forall(a,b,c)\in A^3, (a\cdot b)\cdot c = a\cdot(b\cdot c)$.(Associative)

(iii)- $\forall(a,b,c)\in A^3, a\cdot(b+c) = a\cdot b + a\cdot c$ et $(b+c)\cdot a = b\cdot a + c\cdot a$. (Distrubitive par rapport "+" à gauche et à droite)

Si, de plus: -La propriété suivante est vérifiée : $\forall(a,b)\in A\times A, a\cdot b = b\cdot a$, l'anneau A est dit commutatif.

-Si la loi " $\cdot$ " possède un élément neutre on dit que l'anneau est unitaire et on désigne par 1 (Appelé l'unité de A).

Définition 1.1.2 ***(Sous-anneau)***

Soient A un anneau et B une partie non vide de A.

On dit que B est un sous-anneau de A s'il est un anneau pour les lois de A.

Définition 1.1.3 ***(Idéal)***

Un idéal I d'un anneau A est un sous-groupe de $(A, +)$ tel que I soit stable par la multiplication par les éléments de A, i.e. $x \in I$ et $\lambda \in A \Rightarrow \lambda \cdot x \in I$.

Exemple 1.1.1 *Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ où $n \in \mathbb{Z}$.*

Définition 1.1.4 *Soient A et B deux anneaux unitaires et I idéal de A.*

f un homomorphisme d'anneaux $(A, +, \cdot), (B, \oplus, \odot)$ si:

- $\forall x, y \in A,\ f(x + y) = f(x) \oplus f(y)$.
- $\forall x, y \in A,\ f(x \cdot y) = f(x) \odot f(y)$.
- *Si: A,B sont unitaires:* $f(1_A) = 1_B$.

Proposition 1.1.1 *Soit A un anneau.*

- *On dit que A est intègre s'il n'a pas de diviseur de 0, i.e.si pour a et b dans A, la relation $a \cdot b = 0$ implique $a = 0$ ou $b = 0$.*
- *Soit A un anneau commutatif unitaire et fini:*

  L'ensemble des éléments inversibles de A (Pour la multiplication) se note A^*.

  L'ensemble $(A^*, \cdot)$ est un groupe abélien (Appelé le groupe des unités de A).

Définition 1.1.5 *Soit A un anneau commutatif unitaire et I un idéal de A.*

On définit sur A la relation $\sim$ pour $x, y \in A$:

$$x \sim y \Longleftrightarrow (x - y) \in I \Leftrightarrow x + I = y + I.$$

$\sim$: est une relation d'équivalence c'est-à-dire réflexive et symétrique et transitive.

Définition 1.1.6 ***(Anneau quotient)***

Soit A un anneau, I idéal de A. On définit l'ensemble :

$A/I = \{x+I \ ; \ x \in A\} = \{\overline{x} \ ; \ x \in A\}$ est un anneau commutatif. (On l'appelle l'anneau quotient de A par I) dont les deux opérations sont définies par :

$$\overline{x} + \overline{y} = \overline{x+y}$$

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

Exemple 1.1.2 *$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau intègre si et seulement si n est premier.*

Définition 1.1.7 ***(Corps)***

Un corps (commutatif) $\mathbb{k}$ est un anneau unitaire tel que tout élément non nul est inversible pour la multiplication.

Exemple 1.1.3 *1. $(\mathbb{Q}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{R}, +, \cdot)$ sont des corps (commutatif).*

2. $(\mathbb{Z}, +, \cdot)$ n'est pas un corps.

1.1.2 Corps fini

Définition 1.1.8 ***(Corps fini)***

Un corps $\mathbb{F}$ est fini s'il possède un nombre fini d'éléments, et on le notée $\mathbb{F}_q$ ou $GF(q)$. C'est le ***corps de Galois*** *d'ordre q.*

Notation 1.1.1 *$|\mathbb{F}| = card(\mathbb{F}) =$ ordre de $\mathbb{F}$.*

Exemple 1.1.4 *1. $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps fini si et seulement si p est premier.*

2. $GF(7) = \mathbb{F}_7 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\right\}$ est un corps fini à 7 éléments muni de l'addition $(+)$ et de multiplication $(\cdot)$ modulo 7. Et on a "0" l'élément neutre de l'addition et "1" l'élément neutre de multiplication.

3. $\mathbb{F}_6$ n'est pas un corps fini car : $\overline{2} \times \overline{3} = \overline{6} = \overline{0}$.

1.1.3 Caractéristique d'un corps fini

Définition 1.1.9 *Soit $\mathbb{k}$ un corps, le plus petit entier positif n telle que $n \cdot 1 = 0$ est appelé le caractéristique de $\mathbb{k}, (car(\mathbb{k}) = n)$ sinon on dit que $\mathbb{k}$ est de caractéristique 0.*

Notation 1.1.2

$$n \cdot 1 = \underbrace{1 + ... + 1}_{n\ fois}$$

Exemple 1.1.5 *1.* $\mathbb{F}_p = \left\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{p-1}\right\}$,$car(\mathbb{F}_p) = p$ *telle que* :

$$p \cdot 1 = \underbrace{1 + ... + 1}_{p\ fois} = 0 \quad .$$

2. $car(\mathbb{Q}) = car(\mathbb{R}) = car(\mathbb{C}) = 0$.

Proposition 1.1.2 *Soit $\mathbb{k}$ un corps de caractéristique $n \in \mathbb{N}^*$ et on a $\forall x \in \mathbb{k}$ telle que:*

$$n \cdot x = (n \cdot 1) \cdot x = 0.$$

Théorème 1.1.1 *Soit $\mathbb{k}$ un corps.*

1) Si $car(\mathbb{k}) = 0$, alors $\mathbb{k}$ est infini et $\mathbb{k}$ contient $\mathbb{Q}$ à un isomorphe près.

2) Si $car(\mathbb{k}) = n \neq 0$, alors n est premier et $\mathbb{k}$ contient $(\mathbb{Z}/n\mathbb{Z})$ à un isomorphe près.

Démonstration. Soit l'application :

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{k} \\ n &\to n \cdot 1_{\mathbb{k}} \end{aligned}$$

Soit $n, m \in \mathbb{Z}$ telle que:

- $\varphi(n+m) = 1_{\mathbb{k}} + ... + 1_{\mathbb{k}}; (n+m) fois$

  $\varphi(n+m) = 1_{\mathbb{k}} + ... + 1_{\mathbb{k}}(n\ fois) + 1_{\mathbb{k}} + ...1_{\mathbb{k}}(m\ fois) = n \cdot 1_{\mathbb{k}} + m \cdot 1_{\mathbb{k}}$

  $\varphi(n+m) = \ \varphi(n) + \varphi(m).$

- $\varphi(n \cdot m) = \ (n \cdot m) \cdot 1_{\mathbb{k}} = (n \cdot 1_{\mathbb{k}}) \cdot (m \cdot 1_{\mathbb{k}}) = \varphi(n) \cdot \ \varphi(m).$

- $\varphi(1) = 1_{\Bbbk}$.

Donc φ est un homomorphisme d'anneaux. D'après le premier théorème d'isomorphisme : $ker\varphi$ est un idéal de $\mathbb{Z}$ est $\mathbb{Z}/ker\varphi \simeq \operatorname{Im}\varphi$.
$ker\varphi = \{n \in \mathbb{Z} \ / \ \varphi(n) = 0\} = \{n \in \mathbb{Z} \ / \ n \cdot 1_{\Bbbk} = 0\} = (\ n\ )$ avec $n = car(\Bbbk)$.

1. Si $car(\Bbbk) = 0$ donc, $ker\varphi = \{0\}$, donc $\mathbb{Z}/ker\varphi = \mathbb{Z}/\{0\} = \mathbb{Z} \simeq \operatorname{Im}\varphi \subseteq \Bbbk$. Et on a $\mathbb{Z}$ est infini alors $\Bbbk$ infini.

   $\Bbbk$ est un corps contient $\mathbb{Z}$ à un isomorphe près, donc $\Bbbk$ contient le corps de fractions de $\mathbb{Z}$ à un isomorphe près qui est $\mathbb{Q}$. (puisque le plus petit corps qui contient un anneau est son corps de fraction).

2. Si $car(\Bbbk) = n$ donc, $ker\varphi = n\mathbb{Z}$ donc $\mathbb{Z}/ker\varphi = \mathbb{Z}/n\mathbb{Z} \simeq \operatorname{Im}\varphi \subseteq \Bbbk, \Bbbk$ est un corps, donc $\Bbbk$ intègre, donc $Im\varphi$ est intègre puisque Im $\varphi \subseteq \Bbbk$, donc $\mathbb{Z}/n\mathbb{Z}$ intègre, donc n est premier. Et comme $\mathbb{Z}/n\mathbb{Z} \simeq \operatorname{Im}\varphi$ donc $\Bbbk$ contient $\mathbb{Z}/n\mathbb{Z}$ à un isomorphisme près.

■

Corollaire 1.1.1 *Soit $\mathbb{F}_q$ un corps fini à q éléments, alors :*

1. *$q = p^n$ avec p premier et $n \geq 1$.*
2. *$\forall x \in \mathbb{F}_q : x^q = x$.*

1.1.4 Endomorphisme de Frobenius

Proposition 1.1.3 [**12**] *Soit $\mathbb{F}_q$ et $(q = p^n)$ un corps fini de caractéristique p telle que p est premier alors: $(a+b)^{p^i} = a^{p^i} + b^{p^i}, \forall a, b \in \mathbb{F}_q$ et $i \in \mathbb{N}^*$.*

Théorème 1.1.2 [**12**] *Soit $\Bbbk$ un corps de caractéristique $p > 0$.*

*Notons l'application : (φ s'appelle l'endomorphisme de **Frobenius**).*

$$\begin{aligned} \varphi : \Bbbk &\to \Bbbk \\ x &\to x^p \end{aligned}$$

Alors :

1. *φ est un morphisme de corps (donc injectif).*

2. *Si $\mathbb{k}$ est fini, c'est un automorphisme (i.e.il est bijectif).*

3. *Pour $x \in \mathbb{k}, \varphi(x) = x$ si et seulement si $x \in \mathbb{F}_p$.*

1.2 Existence et unicité des corps finis

1.2.1 Groupe multiplicatif d'un corps fini

Théorème 1.2.1 [13] ***(Théorème de Wedderburn)***

Tout corps fini est commutatif.

Définition 1.2.1 *Soit $\mathbb{k}$ un corps fini de cardinal $q = p^n$. Le groupe multiplicatif $\mathbb{k}^* = \mathbb{k}\backslash\{0\}$ est un groupe cyclique d'ordre $q - 1$.*

Corollaire 1.2.1

- *Soit $q = p^n$, p étant un nombre premier. Alors:*

$$(\mathbb{F}_q^*, \times) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +).$$

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

- *Soit $\mathbb{F}_q$ un corps fini. Alors, tout sous-groupe fini de $\mathbb{F}_q^*$ est cyclique.*

1.2.2 Corps algébriquement clos

Définition 1.2.2 ***(Corps algébriquement clos)***

On dit que le corps commutatif $\mathbb{k}$ est algébriquement clos si tout polynôme non constant possède au moins une racine dans $\mathbb{k}$.

Définition 1.2.3 ***(Extension algébrique)***

Soit $\mathbb{k}$ un corps commutatif :

$\mathbb{k} \subseteq E$ est une extension algébrique si $\forall x \in E$: x est algébrique sur $\mathbb{k}$.

Définition 1.2.4 ***(Clôture algébrique)***

On dit que E est une clôture algébrique de $\mathbb{k}$ *si :*

1-E est une extension algébrique de $\mathbb{k}$*.*

2-E est algébriquement clos.

Exemple 1.2.1 $\mathbb{C}$ *est une clôture algébrique de* $\mathbb{R}$*." C'est le théorème fondamental de l'algébre".*

Théorème 1.2.2 *Un corps fini n'est jamais algébriquement clos.*

Démonstration. Soit $\mathbb{F} = \{x_1, \cdots, x_n\}$ un corps fini. Considérons le polynôme $P(X) = (X - x_1) \cdots (X - x_n) + 1$, c'est un polynôme de degré n et qui vérifie $P(X) = 1 \neq 0$ pour tout $X \in \mathbb{F}$. Donc, $\mathbb{F}$ n'est pas algébriquement clos. ■

Proposition 1.2.1 *Tout corps commutatif* $\mathbb{k}$ *possède une clôture algébrique unique à un isomorphisme près.*

C'est-à-dire :Si E et L deux clôtures algébriques de $\mathbb{k}$ *alors il existe un isomorphisme*

$$f : E \to L \text{ tel que} : \forall x \in \mathbb{k}, f(x) = x$$

Notation 1.2.1 $\overline{\mathbb{k}}$ *désigne la clôture algébrique d'un corps commutatif* $\mathbb{k}$*.*

Remarque 1.2.1 *Si* $\overline{\mathbb{k}}$ *une clôture algébrique de* $\mathbb{k}$ *et L une extension de* $\mathbb{k}$ *alors:*

$$car(\mathbb{k}) = car(L)$$

1.2.3 Existence et unicité des corps finis

Théorème 1.2.3 ***(Existence du corps*** $\mathbb{F}_q$ ***)***

Soient p un nombre premier, $n \in \mathbb{N}^*$*. On pose* $q = p^n$*.*

On considère le polynôme $x^q - x$ *comme à coefficients dans* $\mathbb{F}_p$*. Alors le corps de décomposition du polynôme* $x^q - x$ *sur* $\mathbb{F}_p$ *est un corps à q éléments noté* $\mathbb{F}_q$*.*

Démonstration. Soit p un nombre premier, donc $\mathbb{Z}/p\mathbb{Z}$ est un corps fini à p éléments noté $\mathbb{F}_p$, comme $\mathbb{F}_p$ est un corps, il possède une clôture algébrique noté $\overline{\mathbb{F}_p}$. Soit $\mathbb{k} = \{x \in \overline{\mathbb{F}_p} / x^q - x = 0\}$.

Montrons que $\mathbb{k}$ est un corps (sous corps de $\overline{\mathbb{F}_p}$) :

- $\mathbb{k} \neq 0$ car $0 \in \mathbb{k}$.
- $\forall x, y \in \mathbb{k} : (x-y)^q = x^q - y^q = x - y$, donc $x - y \in \mathbb{k}$.
- $\forall x, y \in \mathbb{k} : (xy)^q = x^q y^q = xy$, donc $xy \in \mathbb{k}$.

Montrons que $|\mathbb{k}| = q$:on remarque que $\mathbb{k}$ est l'ensemble des racines du polynôme : $P(x) = x^q - x$ et $deg(P(x)) = q$ donc $card(\mathbb{k}) \leq q$ et on a $P'(x) = qx^{q-1} - 1 = -1$ car $(qx = p^n x = pp^{n-1}x = 0$ et $p = car(\mathbb{k}))$.
On remarque que toute racine de $P(x)$ n'est pas une racine de $P'(x)$,
donc toutes les racines de $P(x)$ sont simples, donc $P(x)$ admet exactement q racines, alors $|\mathbb{k}| = q$. ■

Théorème 1.2.4 ***(Unicité du corps*** $\mathbb{F}_\mathbf{q}$ ***)***

Soit $\mathbb{k}$ *un corps fini à* $(q = p^n)$ *éléments. Alors il est isomorphe au corps* $\mathbb{F}_q$.
C'est-à-dire deux corps finis ayant le même nombre d'éléments sont isomorphes.

Démonstration. Soit L un autre corps fini à q éléments, donc $car(L) = p$ donc L est une extension de $\mathbb{F}_p$.
On a $\overline{L}$ est aussi une clôture algébrique de $\mathbb{F}_p$ (puisque $\mathbb{F}_p \subset L \subset \overline{L}$) et on a $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$ (déjà choisi).
Donc il existe un isomorphisme $\varphi : \overline{L} \to \overline{\mathbb{F}_p}$ avec $\varphi(x) = x, \forall x \in \mathbb{F}_p$
L est un sous corps de $\overline{L}$, donc $\varphi(L)$ est un sous corps de $\overline{\mathbb{F}_p}$ donc $|L| = |\varphi(L)| = q$.
Comme $\varphi(L)$ est un sous corps de $\overline{\mathbb{F}_p}$, donc $\forall \alpha \in \varphi(L) : \alpha^q - \alpha = 0$, donc $\varphi(L) \subset \mathbb{k}$ et puisque $|\varphi(L)| = q$ donc $\varphi(L) = \mathbb{k}$ alors $\mathbb{k}$ et L sont isomorphes. ■

Corollaire 1.2.2 *Il existe un corps fini* $\mathbb{F}_q$ *à* q *éléments si et seulement si* $q = p^n$ *avec* p *premier et* $n \in \mathbb{N}^*$. *Dans ce cas* $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} / x^q - x = 0\}$.

1.2.4 L'élément primitif

Définition 1.2.5 ***(L'élément primitif)***

Un élément $a \in \mathbb{F}_q$ *qui engendre le groupe cyclique* $\mathbb{F}_q^*$ *est dit primitif.*

Proposition 1.2.2 *Soit a un élément primitif d'un corps fini $\mathbb{F}_q$ alors:*

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

Avec : $a^{q-1} = 1$ de plus a^k est primitif si et seulement si $pgcd(k, q-1) = 1$.

Corollaire 1.2.3 ***(Théorème de l'élément primitif pour les corps finis)***

Toute extension finie d'un corps fini $\mathbb{F}_q$ est une extension simple, i.e. de la forme $\mathbb{F}_q(\alpha)$.

Démonstration. Si $\mathbb{F}_q \subset \mathbb{F}_{q'}$ et si α est un élément primitif de $\mathbb{F}_{q'}$, alors:
$\mathbb{F}_{q'}^* = \{1, \alpha, \alpha^2, ..., \alpha^{q'-2}\}$ donc $\mathbb{F}_{q'} = \mathbb{F}_q(\alpha)$. ■

1.2.5 Sous corps d'un corps fini

Théorème 1.2.5 *Soient $t, s \in \mathbb{N}^*$, on a:*

$$\mathbb{F}_{q^s} \text{ sous corps de } \mathbb{F}_{q^t} \Leftrightarrow s \mid t \text{ dans } \mathbb{N}^*.$$

Démonstration. L'inclusion $\mathbb{F}_{q^s} \subset \mathbb{F}_{q^t}$ entraîne

$$[\mathbb{F}_{q^t} : \mathbb{F}_q] = [\mathbb{F}_{q^s} : \mathbb{F}_q] \cdot [\mathbb{F}_{q^t} : \mathbb{F}_{q^s}] \Rightarrow t = s \cdot [\mathbb{F}_{q^t} : \mathbb{F}_{q^s}]$$

de sorte que s divise t.

Réciproquement, si $s \mid t$ et si $\overline{\mathbb{F}_p}$ désigne une clôture algébrique de $\mathbb{F}_{q^s}$ donc:

$$\mathbb{F}_{q^s} = \{x \in \overline{\mathbb{F}_p} / x^{q^s} - x = 0\}.$$

$$s \mid t \Rightarrow (q^s - 1) \mid (q^t - 1) \Rightarrow (x^{q^{s-1}} - 1) \mid (x^{q^{t-1}} - 1).$$

Si on multiple par x on trouve $(x^{q^s} - x) \mid (x^{q^t} - x)$ donc les racines de $x^{q^s} - x$ sont des racines de $x^{q^t} - x$ alors: $\mathbb{F}_{q^s} \subset \mathbb{F}_{q^t}$. ■

Exemple 1.2.2 *Tous les sous corps de $\mathbb{F}_{7^{12}}$,on a $D(12) = \{1, 2, 3, 4, 6, 12\}$ "l'ensemble des diviseurs de 12."*

Il y a 6 sous corps de $\mathbb{F}_{7^{12}}$ sont $\mathbb{F}_7, \mathbb{F}_{7^2}, \mathbb{F}_{7^3}, \mathbb{F}_{7^4}, \mathbb{F}_{7^6}, \mathbb{F}_{7^{12}}$,et on a 3 chaines :

$$\mathbb{F}_7 \subset \mathbb{F}_{7^2} \subset \mathbb{F}_{7^4} \subset \mathbb{F}_{7^{12}}$$

$$\mathbb{F}_7 \subset \mathbb{F}_{7^2} \subset \mathbb{F}_{7^6} \subset \mathbb{F}_{7^{12}}$$

$$\mathbb{F}_7 \subset \mathbb{F}_{7^3} \subset \mathbb{F}_{7^6} \subset \mathbb{F}_{7^{12}}$$

Représentées par le diagramme suivant :

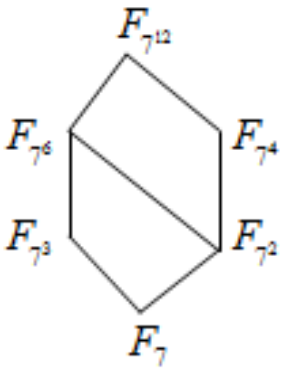

Diagramme de tous les sous corps de $\mathbb{F}_{7^{12}}$

1.2.6 Construction d'un corps fini

Si $f(X) \in \mathbb{F}_p[X]$, on note $(f(X))$ l'idéal de $\mathbb{F}_p[X]$ engendré par $f(X)$.

On appelle un polynôme irréductible est un polynôme qui n'admet pas des diviseurs propres.

Proposition 1.2.3 *Soit p un nombre premier et $f(X)$ un polynôme irréductible de degré n dans l'anneau $\mathbb{F}_p[X]$, alors l'anneau quotient $\mathbb{F}_p[X]/(f(X))$ est un corps fini de cardinal p^n, isomorphe à $\mathbb{F}_{p^n}$.*

Cette proposition nous fournit une représentation des éléments de $\mathbb{F}_{p^n}$ par des polynômes à coéfficient dans $\mathbb{F}_p$ de degré au plus $n-1$ en une racine α de $f(X)$.

Corollaire 1.2.4 *Soit $\mathbb{F}_p$ un corps fini et $f(X) \in \mathbb{F}_p[X]$ un polynôme minimal de α (irréductible unitaire) de degré n. Alors:*

$$\begin{aligned} \mathbb{F}_p[X]/(f(X)) &= \{a_0 + a_1X + a_2X^2 + ...a_{n-1}X^{n-1} + (f(X));\ a_i \in \mathbb{F}_p\} \\ &= \{a_0 + a_1\alpha + a_2\alpha^2 + ...a_{n-1}\alpha^{n-1};\ a_i \in F_p\}. \end{aligned}$$

Est un espace vectoriel sur F_p de dimension n de base $\{1, \alpha, ..., \alpha^{n-1}\}$avec:

$\alpha = \overline{X} = X + (f(X))$ *où* $f(\alpha) = 0$ *et* $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[X]/(f(X))$

Corollaire 1.2.5 *Soit $\mathbb{F}_p$ un corps fini et $f(X) \in \mathbb{F}_p[X]$, de degré n, alors les assertions suivantes sont équivalentes:*

- $f(X)$ *est un polynôme irréductible.*
- $\mathbb{F}_p[X]/(f(X))$ *est un corps.*
- $(f(X))$ *est un idéal maximal.*

Exemple 1.2.3 *Construction de $\mathbb{F}_{49} = \mathbb{F}_{7^2}$. "Corps fini à 49 élément".*

Dans $\mathbb{F}_7$, le polynôme $f(X) = X^2 + X + 3$ est irréductible car il n'admet pas de racines dans $\mathbb{F}_7$. On détermine les éléments de $\mathbb{F}_{7^2}$ en le regardant comme extension obtenue par adjonction à $\mathbb{F}_7$ d'une racine de $f(X)$, ainsi $\mathbb{F}_7[X]/(f(X))$, soit α une racine de $f(X)$, alors $\{1, \alpha\}$est une base de $\mathbb{F}_{7^2}$.

$$\mathbb{F}_7[X]/(f(X)) = \{a_0 + a_1\alpha; a_0, a_1 \in \mathbb{F}_7\}.$$

Dans $\mathbb{F}_7$, c'est-à-dire que : $\alpha^2 = 6\alpha + 4$, et on aura:

$$\mathbb{F}_{7^2} = \mathbb{F}_7[X]/(f(X)) = \{0, 1, \alpha, \alpha^2, ..., \alpha^{47}\}.$$

Donc les éléments de $\mathbb{F}_{49}$ *:*

	comme un polynôme	*comme puissance de* α
00	0	0
10	1	1
01	α	α
46	$4+6\alpha$	α^2
35	$3+5\alpha$	α^3
65	$6+5\alpha$	α^4
61	$6+\alpha$	α^5
45	$4+5\alpha$	α^6
66	$6+6\alpha$	α^7
30	3	α^8
03	3α	α^9
54	$5+4\alpha$	α^{10}
21	$2+\alpha$	α^{11}
41	$4+\alpha$	α^{12}
43	$4+3\alpha$	α^{13}
51	$5+\alpha$	α^{14}
44	$4+4\alpha$	α^{15}
20	2	α^{16}
02	2α	α^{17}
15	$1+5\alpha$	α^{18}
63	$6+3\alpha$	α^{19}
53	$5+3\alpha$	α^{20}
52	$5+2\alpha$	α^{21}
13	$1+3\alpha$	α^{22}
55	$5+5\alpha$	α^{23}
60	6	α^{24}
06	6α	α^{25}
31	$3+\alpha$	α^{26}
42	$4+2\alpha$	α^{27}

12	$1+2\alpha$	α^{28}
16	$1+6\alpha$	α^{29}
32	$3+2\alpha$	α^{30}
11	$1+\alpha$	α^{31}
40	4	α^{32}
04	4α	α^{33}
23	$2+3\alpha$	α^{34}
56	$5+6\alpha$	α^{35}
36	$3+6\alpha$	α^{36}
34	$3+4\alpha$	α^{37}
26	$2+6\alpha$	α^{38}
33	$3+3\alpha$	α^{39}
50	5	α^{40}
05	5α	α^{41}
62	$6+2\alpha$	α^{42}
14	$1+4\alpha$	α^{43}
24	$2+4\alpha$	α^{44}
25	$2+5\alpha$	α^{45}
64	$6+4\alpha$	α^{46}
22	$2+2\alpha$	α^{47}

Chapitre 2

Polynômes irréductibles

Les polynômes irréductibles sur les corps finis ont beaucoup d'applications dans la théorie des nombres et sont souvent utilisés dans la construction des codes correcteurs d'erreurs.

Dans ce chapitre nous allons étudier les polynômes à coefficients dans un corps fini et l'arithmétique sur l'anneau $\mathbb{F}_q[X]$, et la décomposition d'un polynôme en facteurs irréductibles.

2.1 Anneau des polynômes

2.1.1 L'ensemble des polynômes

Définition 2.1.1 ***(Anneau des polynômes)***

Soit A un anneau commutatif unitaire, toute suite d'éléments de A n'ayant qu'un nombre fini de termes non nuls est dite polynôme à coefficients dans A .

L'ensemble des polynômes sur A est noté $A[X]$.

Proposition 2.1.1 *Si $f = (a_0, a_1, ...a_n, 0, 0, ...) \in A[X]$ on notera $f = (a_0, a_1, ...a_n)$*

Si $a_n \neq 0$ on appelle n le degré de f $(n = deg\ f\ )$, Si $a_n = 1$, on dit que f est unitaire.

On pose $deg(0, 0, 0, ...) = -\infty$.

Les polynômes de degré égal à 0 sont les constantes.

2.1.2 Opérations sur A[X]

Définition 2.1.2 ***(L'addition et la multiplication)***

Dans $A[x]$ *on définit l'addition et la multiplication comme suit :*

$(a_0, a_1, ...) + (b_0, b_1, ...) = (a_0 + b_0, a_1 + b_1, ...)$

$(a_0, a_1, ...)\ (b_0, b_1, ...) = (c_0, c_1, ...)$ *où* $c_k = \sum_{i=0}^{i=k} a_i b_{k-i}$.

Proposition 2.1.2 *Soient* A *un anneau commutatif unitaire et* $f, g \in A[X]$.

- $deg(f + g) \leq Max\{\deg(f); \deg(g)\}$. *Avec égalité si et seulement si* $\deg(f) \neq \deg(g)$.
- *Si* A *est intègre alors* $\deg(fg) = \deg(f) + \deg(g)$.

Exemple 2.1.1 *Soient* $f = (1, 2, 3)$ *et* $g = (0, 3, 2, 1) \in \mathbb{Z}/6\mathbb{Z}[X]$.

$fg = (0, 3, 5, 5, 1)$ *donc :*

$$deg(fg) = 4 \neq 5 = \deg(f) + \deg(g)\ \textit{car}\ \mathbb{Z}/6\mathbb{Z}\ \textit{n'est pas intègre.}$$

Corollaire 2.1.1 *Muni des deux opérations* " $+$ " *et* " $\cdot$ " *définies ci-dessus,* $A[X]$*est un anneau commutatif avec unité (1,0,0,.....)*

$(A[X], +, \cdot)$ *est appelé l'anneau des polynômes sur* A .

Dans $A[X]$*, on définit* $X = (0, 1, 0, ...)$, $X^2 = (0, 0, 1, 0....) \ldots$*avec* $X^0 = (1, 0, 0, ...)$.

Ce qui permet d'écrire toute polynôme f de degré n comme suit:

$$f(X) = a_0 + a_1 X + ... + a_n X^n.$$

Définition 2.1.3 ***(Polynôme à coefficients dans un corps fini)***

L'anneau des polynômes $\mathbb{F}_q[X]$ *(ou* $\Bbbk[X]$ *en général,* $\Bbbk$ *corps) est l'ensemble des polynômes* $f(X)$ *à coefficients dans* $\mathbb{F}_q$.

2.2 Arithmétique dans $\mathbb{F}_q[X]$

2.2.1 Division Euclidienne

Définition 2.2.1 ***(Divisibilité)***

Soit $f, g \in \mathbb{F}_q[X]$ *avec* $\deg(f) > 0$. *On dit que* f *divise* g *noté* $(f \mid g)$ *si* $g = fh$ *pour* $h \in \mathbb{F}_q[X]$ *et* $\deg(f) < \deg(g)$.

On dit que f *est un diviseur propre de* g *ou* g *est un multiple de* f.

Exemple 2.2.1 $X + 1$ *divise* $X^2 + X$ *En effet:* $X^2 + X = X(X + 1)$

Théorème 2.2.1 ***(Division Euclidienne)***

Soit $\mathbb{F}_q$ *un corps fini et* $A(X), B(X)$ *deux polynômes de* $\mathbb{F}_q[X], A \neq 0$ *alors il existe un unique couple* $(Q(X), R(X))$ *de* $\mathbb{F}_q[X] \times \mathbb{F}_q[X]$ *tel que :*

$$A(X) = B(X)Q(X) + R(X), \text{ avec } \deg(R) < \deg(B)$$

On dit que Q *est le quotient et* R *le reste de la division euclidienne de* A *par* B.

Exemple 2.2.2 $f(X) = 2X^3 + X^2 + 1, g(X) = X^2 + 2$ *sur* $\mathbb{F}_3[X]$.

$$f(X) = (X^2 + 2)(2X + 1) + 2X + 2.$$

Donc : le quotient $Q(X) = 2X + 1$ *et le reste* $R(X) = 2X + 2$.

Proposition 2.2.1 *Soit* A *et* B *deux polynômes non nuls de* $\mathbb{F}_q[X]$. *On a l'équivalence:*

$$\{(A \text{ divise } B) \text{ et } (B \text{ divise } A)\} \Longleftrightarrow (\exists \lambda \in F_q^*, A = \lambda B).$$

Démonstration. Soit Q et Q' les deux polynômes non nuls tels que :

$A = QB$ et $B = Q'A$, cela donne $A = Q'QA$, l'anneau $\mathbb{F}_q[X]$ étant intègre, on en déduit $Q'Q = 1$, d'où $deg(Q) = 0$. C'est-à-dire qu'il existe $\lambda \in \mathbb{F}_q^*$ tel que $Q = \lambda \in \mathbb{F}_q^*$. ■

Définition 2.2.2 ***(Zéro d'un polynôme)***

On dit que l'élément $\alpha \in \mathbb{F}_q$ *est un zéro (une racine) de* f *dans* $\mathbb{F}_q$ *si* $f(\alpha) = 0$.

Corollaire 2.2.1 *Soit* $f(X) \in \mathbb{F}_q[X]$ *et* $\alpha \in \mathbb{F}_q$ *:*

$$f(\alpha) = 0 \text{ si et seulement si } (X - \alpha) \text{ divise } f.$$

Démonstration. Si $f(X) = (X-\alpha)g(X)$, $g \in \mathbb{F}_q[X]$ on a $f(\alpha) = 0$.

Réciproquement, on suppose que α est un racine de f dans $\mathbb{F}_q$, et en effectuant la division euclidienne de $f(X)$ par $(X-\alpha)$, $\exists! g(X)$, $r(x) \in \mathbb{F}_q[X]$ tel que:

$$f(X) = (X-\alpha)g(X) + r(X) \text{ où } \deg(r(X)) < \deg(X-1) = 1.$$

Alors: $\deg(r(X)) = 0 \Longrightarrow r(X)$ est un polynôme constant.

Et on a $f(\alpha) = 0 \Longleftrightarrow r(X) = 0 \Longrightarrow r(X)$ est un polynôme nul.

Donc $(X-\alpha)$ divise $f(X)$. ■

Définition 2.2.3 ***(Congruence modulo un polynôme)***

Soient $f, g, h \in \mathbb{F}_q[X]$, avec $\deg(h) > 0$.

On dit que $f(X)$ et $g(X)$ sont congrus modulo le polynôme $h(X)$ si $h(X)$ divise $(f(X) - g(X))$, qu'on note:

$$f(X) \equiv g(X) (\mathrm{mod}\, h(X)) \Longleftrightarrow f(X) - g(X) = h(X)p(X), \text{ avec } p(X) \in \mathbb{F}_q[X]$$

Lemme 2.2.1 *Si $h \in \mathbb{F}_q[X]$, avec $\deg(h) > 0$ et $f, g, f', g' \in \mathbb{F}_q[X]$ des polynômes satisfaisent :*

$$\begin{aligned} f(X) &\equiv f'(X) (\mathrm{mod}\, h(X)) \\ g(X) &\equiv g'(X) (\mathrm{mod}\, h(X)) \end{aligned}$$

Alors:

$$\begin{aligned} 1- \quad f(X) + g(X) &\equiv f(X) + g'(X) (\mathrm{mod}\, h(X)) \\ 2- \quad f(X)g(X) &\equiv f'(X)g'(X) (\mathrm{mod}\, h(X)) \end{aligned}$$

2.2.2 Idéaux de $\mathbb{F}_q[X]$

Soit $\mathbb{F}_q[X]$ l'anneau des polynômes sur un corps fini $\mathbb{F}_q$.

Définition 2.2.4 *On appelle idéal de $\mathbb{F}_q[X]$ toute partie non vide I de $\mathbb{F}_q[X]$ tel que:*

1. *I est stable par " + ".*

2. $\forall f \in I$, *et* $\forall g \in \mathbb{F}_q[X]$, $fg \in I$.

Exemple 2.2.3 $\{0\}$ *et* $\mathbb{F}_q[X]$ *sont des idéaux triviaux dans l'anneau* $\mathbb{F}_q[X]$.

Définition 2.2.5 *Soit* P *un polynôme de* $\mathbb{F}_q[X]$. *On définit l'idéal engendré par* P, *noté* (P) *par*:

$$(P) = \{PQ, Q \in \mathbb{F}_q[X]\}$$

C'est donc l'ensemble des polynômes multiples de P.

Définition 2.2.6 ***(Idéal principal)***

Soit I un idéal de $\mathbb{F}_q[X]$. *On dit que I un idéal principal s'il existe un polynôme P dans* $\mathbb{F}_q[X]$ *tel que* $I = (P)$.

Théorème 2.2.2 [**5**] *Tout idéal de* $\mathbb{F}_q[X]$ *est principal. On dit donc que l'anneau* $\mathbb{F}_q[X]$ *est principal.*

Démonstration. Soit I un idéal de $\mathbb{F}_q[X]$.

Si $I = \{0\}$, alors $I = (0)$.

Supposons que $I \neq \{0\}$ alors $I - \{0\} \neq \phi$. Soit G un polynôme de $I - \{0\}$vérifiant :

$$\deg(G) = \min\{\deg(P) \in \mathbb{N};\ P \in I - \{0\}\}$$

Sachant que $G \in I$ équivant à $(G) \subset I$.....(1)

Soit $A \in I$ par la division Euclidienne, il existe un unique couple de polynômes (Q, R) tel que:

$$A = GQ + R \text{ et } deg(R) < \deg(G).$$

Comme G et A sont des éléments de I, et que I est un idéal , on a:

$$R = A - GQ \in I$$

De:

$$R \in I,\ \deg(G) = \min\{\deg(P) \in \mathbb{N};\ P \in I - \{0\}\} \text{ et } deg(R) < \deg(G).$$

On déduit :

$$R = 0.$$

D'où:

$$A = GQ.$$

Et donc $I \subset (G)$.....(2)

De (1) et (2) : $I = (G)$. ■

Définition 2.2.7 ***(PGCD)***

Si A et B sont deux polynômes de $\mathbb{F}_q[X]$, on dit que le polynôme D est un plus grand commun diviseur (en abrégé, pgcd) de A et B quand:

1. *D est un diviseur commun de A et B.*
2. *Tout diviseur commun de A et B divise D.*

Et on noté $D = pgcd(A, B)$.

Proposition 2.2.2 ***(Polynômes premiers entre eux)***

On dira que deux polynômes A et B sont premiers entre eux si leur seul diviseur unitaire commun est le polynôme 1, autrement dit si leur pgcd est le polynôme 1.

Exemple 2.2.4 *Dans F_3 : $pgcd(X^4 + 1, X^3 + X + 1) = X^2 + X - 1$.*

Dans F_5 : $pgcd(X^4 + 1, X^3 + X + 1) = 1$. Donc $X^4 + 1$ et $X^3 + X + 1$ sont premiers entre eux.

2.2.3 Théorème de Bézout et de Gauss

Théorème 2.2.3 ***(Théorème de Bézout)***

Soit A et B deux polynômes de $\mathbb{F}_q[X]$.

1. *Soit D un diviseur commun unitaire de A et B. Alors D est le pgcd de A et B si et seulement s'il existe deux polynômes U et V de $\mathbb{F}_q[X]$ tels que:*

$$AU + BV = D.$$

2. *En particulier, les polynômes A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V de $\mathbb{F}_q[X]$ tels qu'on ait:*

$$AU + BV = 1.$$

Lemme 2.2.2 ***(Lemme de Gauss)***

Soient A, B et C trois polynômes de $\mathbb{F}_q[X]$*. Si A divise le produit BC et est premier avec B, alors A divise C.*

2.2.4 Algorithme d'Euclide

Proposition 2.2.3 *Soit A et B deux polynômes de* $\mathbb{F}_q[X]$*, avec* $B \neq 0$*, et soit R le reste de la division euclidienne de A par B, alors:*

$$pgcd(A, B) = pgcd(B, R).$$

Définition 2.2.8 *Soient A et B deux polynômes de* $\mathbb{F}_q[X]$*, avec* $B \neq 0$*. On calcule les divisions euclidiennes successives.*

$$A = BQ_1 + R_1, \ \textit{avec} \ \deg(R_1) < \deg(B)$$

$$B = R_1Q_2 + R_2, \ \textit{avec} \ \deg(R_2) < \deg(R_1)$$

$$R_1 = R_2Q_3 + R_3, \ \textit{avec} \ \deg(R_3) < \deg(R_2)$$

$$\vdots$$

$$\vdots$$

$$R_{n-2} = R_{n-1}Q_n + R_n, \ \textit{avec} \ \deg(R_n) < \deg(R_{n-1})$$

$$R_{n-1} = R_nQ_{n+1}.$$

Exemple 2.2.5 *Utiliser l'algorithme d'Euclide. (on travaille dans* F_2*).*

$X^5 + X^4 + 1 = (X^4 + X^2 + 1)(X + 1) + X^3 + X^2 + X$

$X^4 + X^2 + 1 = (X^3 + X^2 + X)(X + 1) + X^2 + X + 1$

$X^3 + X^2 + X = (X^2 + X + 1)X + 0$

Donc: $pgcd(X^5 + X^4 + 1, X^4 + X^2 + 1) = X^2 + X + 1$.

2.3 Polynôme irréductible

2.3.1 Généralité des polynômes irréductibles sur un corps fini

Définition 2.3.1 *Soit $f, g \in \mathbb{F}_q[X]$, on dit que $f(X)$ et $g(X)$ sont associés si:*

$$g(X) = af(X), a \in \mathbb{F}_q^*.$$

Définition 2.3.2 ***(Polynôme irréductible)***

Soit $f(X) \in \mathbb{F}_q[X]$, on dit que $f(X)$ est irréductible:

1. *Si* $\deg(f) > 0$.
2. *Si l'égalité $f(X) = g(X)h(X)$ implique que $g(X) \in \mathbb{F}_q^*$ ou $h(X) \in \mathbb{F}_q^*$.*

Remarque 2.3.1 **(i)-** *Un polynôme irréductible f est donc un polynôme non constant dont les seuls diviseurs de f sont les constantes et f lui-même.*

(ii)- *La notion de polynômes iiréductibles pour l'arithmétique de $\mathbb{F}_q[X]$ correspond à la notion de nombre premier pour l'arithmétique de $\mathbb{Z}$.*

(iii)- *Dans le cas contraire, on dit que f est réductible, il existe alors des polynômes g, h de $\mathbb{F}_q[X]$ tels que $f = gh$ avec* $\deg(g) \geq 1$ *et* $\deg(h) \geq 1$.

Exemple 2.3.1

- *Tout polynôme f de degré* 1 *est irréductible dans $\mathbb{F}_q[X]$.*
- $X^2 + 1 = (X + 1)(X + 1) \in \mathbb{F}_2[X]$ *est réductible.*

Proposition 2.3.1 *Pour tout p premier, il existe des polynômes irréductibles sur $\mathbb{F}_p$ de tous degrés.*

Théorème 2.3.1 *Un polynôme f de degré 2 ou 3 est irréductible dans $\mathbb{F}_q[X]$ (ou $\Bbbk[X]$ en général, $\Bbbk$ corps) si et seulement s'il n'admet pas de racine sur $\mathbb{F}_q$.*

Démonstration. Un polynôme f est réductible si et seulement si s'il possède un diviseur propre , c'est-à-dire un diviseur g vérifiant: $1 \leq \deg(g) \leq \deg(f)$.

Ce qui implique $\deg(f) \geq 2$. Si l'on écrit $f = gh$, on obtient :

$$1 \leq \deg(h) < \deg(f) \text{ et } \deg(g) + \deg(h) = \deg(f)$$

Si $\deg(f) \leq 3$, on en déduit $(\deg(g) = 1)$ ou $(\deg(h) = 1)$, donc f admet une racine. ■

Exemple 2.3.2 *1.* $f(X) = X^2 + X + 1$ *est irréductible dans* $\mathbb{F}_2[X]$.

2. $g(X) = X^2 + X + 4$, $h(X) = X^2 + 6X + 6, k(X) = X^3 + X^2 + 1, l(X) = X^3 + X^2 + 3$, *sont irréductibles dans* $\mathbb{F}_7[X]$.

Lemme 2.3.1 ***(lemme d'Euclide)***

Soit $f \in \mathbb{F}_q[x]$ *un polynôme irréductible et soient* $g, h \in \mathbb{F}_q[x]$. *Si* $f \mid gh$ *alors* $f \mid g$ *ou* $f \mid h$.

Démonstration. Si f ne divise pas g alors $\text{pgcd}(f, g) = 1$ car f est irréductible. Donc par le lemme de Gauss, f divise h. ■

Théorème 2.3.2 [**5**] *Soit* $f(X) \in \mathbb{F}_q[X]$ *un polynôme irréductible de degré m. Alors* $f(X)$ *possède une racine* α *dans* $\mathbb{F}_{q^m}$. *De plus les racines de* $f(X)$ *sont simples et sont données par les éléments distincts suivants* $\{\alpha, \alpha^q, \alpha^{q^2}, ...\alpha^{q^{m-1}}\}$*des éléments de* $\mathbb{F}_{q^m}$ *qui sont appelés les conjugés de* α *pour* $\mathbb{F}_q$.

Remarque 2.3.2 *Si* α *est un élément primitif de* $\mathbb{F}_{q^m}$, *alors ses conjugés sont aussi des éléments primitifs. On dira alors que* $f(X)$ *est un polynôme primitif.*

2.3.2 Décomposition en facteurs irréductibles

Proposition 2.3.2 *Tout polynôme* $f \in \mathbb{F}_q[x]$ *de degré* $n \geq 1$ *admet un factor irréductible.*

Théorème 2.3.3 ***(Décomposition en facteurs irréductibles)***

Tout polynôme $f \in \mathbb{F}_q[x]$ *peut s'écrire*

$$f = a f_1^{e_1} f_2^{e_2} ... f_k^{e_k},$$

où $a \in \mathbb{F}_q$, *les* f_i *sont des polynômes irréductibles unitaires de* $\mathbb{F}_q[x]$ *et les exposants* e_i *des entiers positifs.*

Cette factorisation est unique à ordre des facteurs prés.

Factorisation de $X^{p^n} - X$ sur un corps fini

Proposition 2.3.3 *Soit $f(X) \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n. Le polynôme $f(X)$ est un diviseur de $X^q - X$, où $q = p^n$.*

Théorème 2.3.4 [5] ***(Fondamental)***

Sur $\mathbb{F}_p[X]$, la décomposition en facteurs irréductibles de $X^q - X, q = p^n$, est :

$$X^q - X = \prod_{\substack{f \text{ irréductible} \\ \deg(f)|n}} f(X)$$

Corollaire 2.3.1 *Les facteurs irréductibles sur $\mathbb{F}_p$ de $X^q - X$ sont les polynômes irréductibles de $\mathbb{F}_p[X]$ de degré n, ainsi que les polynômes irréductibles de degré d, pour tout diviseur d de n.*

Exemple 2.3.3 *Dans $\mathbb{F}_2[X]$:*

$$X^8 + X = X^{2^3} + X = X(X^7 + 1) = X(X + 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1).$$

On remarque que:

$$(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1) = (X^3 + X^2 + 1)(X^3 + X + 1).$$

Finalement, $X^8 - X$ s'écrit sous forme de produits de facteurs irréductibles :

$$X^8 - X = X(X + 1)(X^3 + X^2 + 1)(X^3 + X + 1).$$

Il existe donc deux polynômes irréductibles de degré 3 sur $\mathbb{F}_2[X]$:
$P_1(X) = X^3 + X^2 + 1$ et $P_2(X) = X^3 + X + 1$.

2.3.3 Factorisation de $X^n - 1$ sur un corps fini

La factorisation du polynôme $X^n - 1$ joue un rôle important dans la recherche des codes cycliques de longueur n définis sur $\mathbb{F}_q$. 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 $\mathbb{F}_q$:

$$X^n - 1 = \prod_i f_i(X)$$

La factorisation de $X^n - 1$ s'écrit :

$$X^n - 1 = (X-1)f_1.f_2...f_r \text{ avec } \sum_{i=1}^{r} \deg(f_i) = n-1$$

Si $f_i(X) = a_0 + a_1X + a_2X^2 + ... + a_kX^k \Longrightarrow \deg(f_i) = k$ où les f_i sont des polynômes irréductibles sur $\mathbb{F}_q$.

Les racines n-ièmes de l'unité

Soit $\mathbb{F}_q$ un corps fini de caractéristique p et $n = mp^h$, avec $pgcd(m,p) = 1$, alors le polynôme $X^n - 1$ admet la décomposition suivante :

$$X^n - 1 = X^{mp^h} - 1 = (X^m - 1)^{p^h}$$

Pour cela on se restreint au cas où n et q sont premiers entre eux.

On dénote par $\mathbb{F}_{q^s}$ le corps de décomposition de $X^n - 1$ sur $\mathbb{F}_q$, c'est l'extension de $\mathbb{F}_q$ qui contient toutes les racines du polynôme $X^n - 1$.

Comme pgcd$(n,q) = 1$, la dérivée de $X^n - 1$est égale à nX^{n-1} et donc $X^n - 1$ n'a aucune racine double, donc il admet n racines distinctes dans $\mathbb{F}_{q^s}$.

Ces racines sont appelées **racines n-ièmes de l'unité** sur $\mathbb{F}_q$, elles forment le sous groupe E^n de $\mathbb{F}_{q^s}^*$ de cardinal n.

Comme $\mathbb{F}_{q^s}^*$ est cyclique alors E^n est cyclique d'ordre n. Un élément primitif de E^n est appelé **racine primitive n-ième de l'unité**.

Donc si α est une racine primitive n-ième de l'unité, on a alors :

$$\alpha \in \mathbb{F}_{q^s} \Rightarrow \alpha^{q^s} = \alpha \Rightarrow \alpha^{q^s} - 1 = 1 \Rightarrow n|(q^s - 1).$$

L'entier s est appelé l'ordre de q modulo n, c'est le plus petit entier qui vérifie: $q^s \equiv 1 \ mod\ n$.

Exemple 2.3.4

- *Dans $\mathbb{F}_2$ on a:*

$$X^7 - 1 = (X+1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

- *Dans $\mathbb{F}_7$ on a:*

$$X^6 - 1 = (X+1)(X+2)(X+3)(X+4)(X+5)(X+6).$$

Chapitre 3

Codes cycliques optimaux de rendement 1/2 sur GF(7)

Nous rappelons, dans ce chapitre, quelques notions de base sur la théorie des codes.

On commence par donner la définition de code, les codes linéaires et leurs paramétres, les codes cycliques et la construction des codes cycliques, et nous considérons les codes

cycliques optimaux de rendement 1/2 sur le corps fini $\mathbb{F}_7$, et en utilisant l'algorithme de **Chen** pour calculer la distance minimale pour n pair non multiple de 7 et inférieur ou égale à 50.

3.1 Généralités sur les codes

$\mathbb{F}_q$ corps fini à q élément, pour $n \in \mathbb{N}^*$:

$$\mathbb{F}_q^n = \underbrace{\mathbb{F}_q \times \mathbb{F}_q \times ..... \times \mathbb{F}_q}_{n \text{ fois}} = \{(x_1, x_2, ..., x_n); x_i \in \mathbb{F}_q\}.$$

Est un espace vectoriel de dimension n sur $\mathbb{F}_q$ et $\{e_1 = (1, 0, ..., 0), e_2 = (0, 1, 0, ..., 0), ..., e_n = (0, ..., 0, 1)\}$ est une base de $\mathbb{F}_q^n$.

Définition 3.1.1 ***(Un code de longueur n)***

Un code de longueur n sur $\mathbb{F}_q$ est une partie non vide de $\mathbb{F}_q^n$.

Notation 3.1.1

- *Pour $x \in \mathbb{F}_q^n$: x est appelé vecteur ou mot de longueur n sur $\mathbb{F}_q$.*

$$x = (x_1, x_2, ..., x_n) = x_1 x_2 .... x_n.$$

- *Si $c \in C$ (code): c mot de code.*
- *$M = card(C) =\mid C \mid$.*

Exemple 3.1.1

1. *$\mathbb{F}_2 = \{0, 1\}$, $C = \{(0,0,0,0,0), (0,1,0,1,0), (1,0,1,0,1)\} \subset \mathbb{F}_2^5$.*

   C: code de longueur 5 sur $\mathbb{F}_2$ et $M = 3$.

2. *$\mathbb{F}_3 = \{0, 1, 2\}$, $C' = \{(0,2,1), (2,1,1), (1,1,1), (2,0,2)\} \subset \mathbb{F}_3^3$.*

   C': code de longueur 3 sur $\mathbb{F}_3$ et $M = 4$.

3.1.1 Distance de Hamming

Définition 3.1.2 ***(Distance de Hamming)***

Soit $x, y \in \mathbb{F}_q^n$, la distance de Hamming entre x et y est le nombre positif $d_H(x, y)$ définie par:

$$d_H(x, y) =\mid \{i; 1 \leq i \leq n \text{ et } x_i \neq y_i\} \mid .$$

Exemple 3.1.2

- *$x = 1201, y = 0202 \in \mathbb{F}_3^4$, donc $d_H(1201, 0202) = 2$.*
- *$x = 36214, y = 52204 \in \mathbb{F}_7^5$, donc $d_H(36214, 52204) = 3$.*

Proposition 3.1.1 *La distance de Hamming :*

$$d_H : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{N}$$

Vérifie bien les propriétés useulles d'une distance:

- $d_H(x, y) = 0 \Longleftrightarrow x = y$.
- $d_H(x, y) = d_H(y, x)$.
- $d_H(x, z) \leq d_H(x, y) + d_H(y, z)$.

Corollaire 3.1.1 *L'espace métrique $(\mathbb{F}_q^n, d_H)$ est appelé l'espace de Hamming.*

Définition 3.1.3 ***(Le poids de Hamming)***

Soit $x \in \mathbb{F}_q^n$, le poids de Hamming de x, noté $w_H(x)$ est défini par:

$$w_H(x) = \mid \{i; 1 \leq i \leq n \text{ et } x_i \neq 0\} \mid .$$

Exemple 3.1.3 *$x = 030204 \in \mathbb{F}_5^6$, donc $w_H(x) = 3$.*

Remarque 3.1.1 *Soit $x, y \in \mathbb{F}_q^n$, on a :*

$$w_H(x - y) = d_H(x, y).$$

3.1.2 Distance minimale d'un code

C un code de longueur n sur $\mathbb{F}_q$.

Définition 3.1.4 *La distance minimale du code C est l'entier $d(C)$ définie par:*

$$d(C) = \min\{d(x, y); x \neq y \text{ et } x, y \in C\}$$

Exemple 3.1.4 *Soit $C = \{100101, 010110, 111001\} \subset \mathbb{F}_2^6$, donc $d(C) = \min\{3, 3, 4\} = 3$.*

3.1.3 Paramètres d'un code

On note par $[n, M, d]_q$ un code C de longueur n, de cardinal M et de distance minimale d.

3.2 Codes linéaires sur un corps fini

3.2.1 Code linéaire

Définition 3.2.1 ***(Code linéaire)***

Un code linéaire est un $\mathbb{F}_q$-sous-espace vectoriel de l'espace vectoriel $\mathbb{F}_q^n$ de dimension k

Exemple 3.2.1 *1. $\{0\}, \mathbb{F}_q^n$ sont des codes linéaires dits triviaux.*

2. Dans $\mathbb{F}_3^3$ *le code linéaire engendré par* $(1,0,2)$ *et* $(1,1,2)$ *sur* $\mathbb{F}_3$ *est:*

$$C = \{000, 102, 112, 201, 221, 211, 020, 122, 010\}$$

Remarque 3.2.1 *Si C linéaire, on peut remarquer que, si x et y sont dans C, alors* $x - y$ *est également dans C. Comme* $w(x-y) = d(x,y)$*, la distance minimale de C est égale au minimum des poids des éléments non nuls de C. On a:*

$$d(C) = w(C) = \min\{w(x), x \in C \setminus 0\}$$

Exemple 3.2.2 *Dans* $\mathbb{F}_2^4$ *le code linéaire C:*

$$C = \{0000, 1001, 1010, 0011\},\ \textit{Donc}\ d(C) = 2.$$

Proposition 3.2.1 *C est un code linéaire. Si* $\dim_{F_q} C = k$ *alors* $M = q^k$*. Est noté C est un code linéaire de* $[n,k,d]$ *sur* $\mathbb{F}_q$*.*

3.2.2 Matrice génératrice d'un code linéaire

Définition 3.2.2 ***(Matrice génératrice)***

Une matrice génératrice d'un code linéaire C de longueur n et de dimension k est une matrice notée généralement G de type (k,n) *et à coefficients dans* $\mathbb{F}_q$ *dont les lignes forment une base de C.*

Remarque 3.2.2 *Un code posséde en général plusieurs matrices génératrices.*

Exemple 3.2.3 *Soit* $C = \{000, 101, 011, 110\}$ *un code linéaire.*

$\{101, 011\}, \{101, 110\}, \{011, 110\}$ *sont des bases de C.*

Et on a G_1, G_2, G_3 *sont des matrices génératrices de C tels que:*

$$G_1 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, G_3 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

Proposition 3.2.2 *Soit φ l'application définie par:*

$$\begin{aligned} \varphi : \quad & \mathbb{F}_q^k \to \mathbb{F}_q^n \\ & m \to mG \end{aligned}$$

Alors :

1. *φ est une application linéaire injective.*

2. *$C = \operatorname{Im}\varphi = \{mG; m = (m_1, m_2, ..., m_k) \in \mathbb{F}_q^k\}$.*

Exemple 3.2.4 *Soit C le code linéaire de matrice génératrice G sur $\mathbb{F}_q$, $G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$, $k = 2, n = 4$.*

$$C = \{mG; m \in \mathbb{F}_2^2\} = \{00G, 01G, 10G, 11G\} = \{0000, 0110, 1010, 1100\}.$$

3.2.3 Dual d'un code linéaire

Définition 3.2.3 ***(Produit scalaire)***

Soient $x = x_1x_2....x_n$, $y = y_1y_2....y_n \in \mathbb{F}_q^n$.
$\langle x, y\rangle = \sum_{i=1}^{i=n} x_iy_i = x_1y_1 + x_2y_2 + ... + x_ny_n$.
Si $\langle x, y\rangle = 0$, on dit que x et y sont orthogonaux est noté par $x \perp y$.

Définition 3.2.4 ***(Dual d'un code linéaire)***

C un $[n, k]$ code linéaire sur $\mathbb{F}_q$, le dual (l'orthogonal) de C est:

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

$y \in C^\perp \iff \forall x \in C, \langle x, y\rangle = 0$.

Proposition 3.2.3 *Si C un $[n, k]$ code linéaire sur $\mathbb{F}_q$, alors $C^\perp$ est un $[n, n-k]$ code linéaire sur $\mathbb{F}_q$.*

Remarque 3.2.3 *Si $C = C^\perp$, C: est dit auto-dual.*

3.2.4 Matrice de contrôle d'un code linéaire

Définition 3.2.5 *Une matrice de contrôle H d'un code linéaire C de paramètres $[n,k]$ est une matrice génératrice de son dual $C^{\perp}$ et $H \in M_{n-k,n}(\mathbb{F}_q)$.*

Proposition 3.2.4 *Soit C un $[n,k]$ code linéaire sur $\mathbb{F}_q$, G et H respectivement une matrice génératrice et une matrice de contrôle de C.*

- *Alors:*
$$G^t H = 0, H^t G = 0, \text{ où } {}^tG \text{ est la matrice transposée de } G$$
- $x \in C \Longleftrightarrow x^t H = 0 \Longleftrightarrow H^t x = 0$, *car il existe* $m \in \mathbb{F}_q^k$, $x = mG$.

Remarque 3.2.4 *Un code linéaire C de poids d si et seulement si, il existe d colonnes de sa matrice de contrôle de parité linéairement dépendantes, tendis que d-1 colonnes quelconques sont indépendantes.*

3.2.5 Codes systématiques

Définition 3.2.6 ***(Code systématique)***

On dit que C est un code systématique s'il existe une matrice B à coefficients dans $\mathbb{F}_q$, ayant k lignes et $n-k$ colonnes, telle que $(I_k \mid B)$ soit une matrice géénératrice de C.

Proposition 3.2.5 *Soit C un code systématique. Soit $G = (I_k \mid B)$ la matrice génératrice de C.*

Alors, la matrice:
$$H = (-{}^tB | I_{n-k})$$
est une matrice de contrôle de C.

Exemple 3.2.5 *Soit G la matrice génératrice de C sur $\mathbb{F}_3$:*
$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$
Alors, H est une matrice de contrôle de C sur $\mathbb{F}_3$:
$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$$

3.3 Codes cycliques sur un corps fini

3.3.1 Code cyclique

Définition 3.3.1 ***(Code cyclique)***

Un code linéaire C de longueur n sur $\mathbb{F}_q$ est dit cyclique si l'ensemble de ses mots est invariants par décalage circulaire à droite :

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

Exemple 3.3.1 *1. Les codes triviaux $\{0\}$ et $\mathbb{F}_q^n$ sont cycliques.*

2. Le code binaire $C = \{000, 101, 011, 110\}$ est un code cyclique.

3. Le code binaire $C = \{0000, 1001, 0110, 1111\}$ n'est pas cyclique.

3.3.2 Description algébrique des codes cycliques

Tout mot $c = (c_0, c_1, ..., c_{n-1})$ d'un code C sur $\mathbb{F}_q$ peut être identifié à un polynôme:

$$c(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in \mathbb{F}_q[X]$$

Pour pouvoir construire des codes cycliques, l'anneau à considérer est $R_n = \mathbb{F}[X]/(X^n - 1)$.

En effet, dans cet anneau, on peut réduire tout polynôme modulo $X^n - 1$ en remplaçant simplement X^n par $1, X^{n+1}$ par X et ainsi de suite. Le code $C(X)$ est alors un sous ensemble de R_n. Observons ce qui se passe lorsque l'on multiplie $c(X)$ par X dans R_n :

$$\begin{aligned} Xc(X) &= c_0X + c_1X^2 + \cdots + c_{n-1}X^n \\ &= c_{n-1} + c_0X + c_1X^2 + \cdot \cdot \cdot + c_{n-2}X^{n-1}. \end{aligned}$$

La multiplication par X correspond à un décalage circulaire. La multiplication par X^m correspond à m décalages circulaires.

On peut donc traduire la cyclicité d'un code C en concidérant l'ensemble C(X) des polynômes associés aux mots du code C et en demandant que cet ensemble C(X) soit fermé pour les deux opérations suivantes :

(i)- Si $c_1(X)$ et $c_2(X) \in C(X) \subset \mathbb{F}_q[X]$ alors $c_1(X) + c_2(X) \in C(X)$ (linéarité).

(ii)- Si $c(X) \in C(X)$ alors $Xc(X) mod(X^n - 1)$ est encore dans $C(X)$ (cyclicité).

Ce qui précède se résume en disant que l'image de $C(X)$ dans l'anneau $R_n = \mathbb{F}_q[X]/(X^n - 1)$ est un idéal de R_n.

Théorème 3.3.1 [**2**] *C est cyclique si et seulement si $C(X)$ est un idéal de $\mathbb{F}_q[X]/(X^n - 1)$.*

3.3.3 Polynôme générateur et polynôme de contrôle

Définition 3.3.2 ***(Polynôme générateur)***

Le polynôme unitaire ainsi associé à un code linéaire cyclique C est appelé polynôme générateur du code cyclique.

Proposition 3.3.1 *Le polynôme générateur est unique.*

Preuve. Supposons que g_1 et g_2 soient deux polynôme générateurs. Alors $g_1 - g_2$ est un polynôme générateur (le code est linéaire) de degré strictement inférieur au degré des g_i. Contradiction. ■

Proposition 3.3.2 *Tout mot d'un code cyclique est un multiple du polynôme générateur. On note $C = (g)$.*

Preuve. Soit $c(X) \in C$ on effectue la division euclidienne de $c(X)$ par $g(X)$:

$c(X) = a(X)g(X) + r(X)$ avec $deg(r(X)) < deg(g(X))$. Où, le reste $r(X)$ qui est la différence de deux mots du code appartient au code. Si $r(X) \neq 0$, on contredit l'hypothese sur le degré minimum de $g(X)$. ■

Proposition 3.3.3 *Le polynôme générateur divise $X^n - 1$.*

Preuve. On a $X^n - 1 = ag + r$ avec $deg(r) < deg(g)$ et on conclut comme précédemment que r doit être nul (après réduction modulo $X^n - 1$). ■

Proposition 3.3.4 *La dimension k du code cyclique C est $n - r$, où $r = deg(g)$.*

Preuve. Tout mot du code peut être vu comme un polynôme de degré au plus $n-1$, multiple d'un polynôme de degré $deg(g)$. Ces polynômes peuvent donc s'écrire sous la forme $g(X).h(X)$ pour $deg(h) \leq n-1-deg(g)$, il y a donc exactement $q^{n-deg(g)}$ mots possibles qui par constructions sont tous distincts et donc la dimension du code est$k = n - deg(g)$.

Réciproquement, tout polynôme unitaire $g(X)$ de degré $n-k$, divisant X^n-1 est le polynôme générateur d'un code cyclique de longueur n et de dimension k. ■

Remarque 3.3.1 *D'après ce qui précède, il découle que pour déterminer les codes cycliques de longueur n de dimension k sur un corps $\mathbb{F}_q$, il suffit de déterminer les polynômes unitaires de degré $n-k$ divisant X^n-1 dans $\mathbb{F}_q[X]$.*

Exemple 3.3.2 *Soit le code $C = (1+X^2)$ dans $\mathbb{F}_2[X]/(X^3-1)$.*

L'éléments de C sont $0, 1+X, 1+X^2, X+X^2$.

Donc : $C = \{000, 110, 101, 011\}$.

Définition 3.3.3 ***(Polynôme de contrôle)***

Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$, de polynôme générateur g. On appelle polynôme de contrôle de C le polynôme h tel que:

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

Comme g est unitaire de degré $n-k$, le polynôme de contrôle h est unitaire de degré k.

Réciproquement, tout polynôme unitaire h de degré k, divisant X^n-1 est le polynôme de contrôle d'un code cyclique de longueur n et de dimension k.

3.3.4 Représentation matricielle

Soit C un code cyclique de longueur n et de dimension k sur $\mathbb{F}_q$.

Soient $g = \sum_{i=0}^{r} g_i X^i$ et $h = \sum_{i=0}^{k} h_i X^i$ respectivement le polynôme générateur et le polynôme de contrôle de C. On a vu que tout mot $c \in C$ peut s'obtenir en multipliant g (de degré r) par un polynôme a sans avoir à réduire modulo X^n-1 : $c(X) = a(X)g(X)$. Puisque $deg(c(X)) < n$ et $deg(g(X)) = r$, on obtient $deg(a(X)) < n-r$.

Utilisons maintenant la notation matricielle. On a : $c = aG$ où $c = (c_0, ..., c_{n-1})$, $a = (a_0, ..., a_{n-r})$ et G est une matrice circulaire $k \times n$ donnée par :

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & .. & g_r & 0 & .. & .. & .. & 0 & 0 \\ 0 & g_0 & g_1 & g_2 & .. & g_r & 0 & .. & .. & .. & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & .. & g_r & 0 & .. & .. & 0 \\ : & : & : & : & : & : & : & : & : & : & : \\ : & : & : & : & : & : & : & : & : & : & : \\ : & : & : & : & : & : & : & : & : & : & : \\ 0 & 0 & 0 & .. & .. & 0 & g_0 & g_1 & g_2 & .. & g_r \end{pmatrix}$$

G est appelée **matrice génératrice** du code C de longueur n et de dimension $k = n - r$ où $r = deg(g(X))$.

Une **matrice de contrôle** du code C est donnée par :

$$H = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & .. & h_0 & 0 & .. & .. & .. & 0 & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & .. & h_0 & 0 & .. & .. & .. & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & .. & h_0 & 0 & .. & .. & 0 \\ : & : & : & : & : & : & : & : & : & : & : \\ : & : & : & : & : & : & : & : & : & : & : \\ : & : & : & : & : & : & : & : & : & : & : \\ 0 & 0 & 0 & .. & .. & 0 & h_k & h_{k-1} & h_{k-2} & .. & h_0 \end{pmatrix}$$

3.3.5 Dual d'un code cyclique

Définition 3.3.4 ***(Polynôme réciproque)***

Soit f(x) un polynôme de degré n on définit son polynôme réciproque par:

$$f^*(X) = X^n f(X^{-1}) = X^n f(\frac{1}{X}).$$

Proposition 3.3.5 *Soit C un code cyclique de dimension k engendré par le polynôme g(X) de degré r, alors le code $C^\perp$ dual de C est un code cyclique engendré par :*

$$g^\perp(X) = h^*(X) = X^k h(X^{-1}), \text{ avec } h(X) = \frac{X^n - 1}{g(X)}.$$

Exemple 3.3.3 *Déterminons les codes cycliques binaires de longueur* 7.

La factorisation en produit de polynômes irréductibles de $X^7 - 1$ *sur* $\mathbb{F}_2$ *est:*

$$X^7 - 1 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

On obtient alors $2^3 = 8$ *codes cycliques binaires de longueur* 7, *dont, par exemple :*

- *Le code* C_1 *engendré par* $g_1(X) = 1$.
- *Le code* C_2 *engendré par* $g_2(X) = X + 1$.
- *Le code* C_3 *engendré par* $g_3(X) = X^3 + X + 1$.
- *Le code* C_4 *engendré par* $g_4(X) = X^3 + X^2 + 1$.
- *Le code* C_5 *engendré par* $g_5(X) = (X - 1)(X^3 + X + 1) = X^4 + X^3 + X^2 + 1$.
- *Le code* C_6 *engendré par* $g_6(X) = (X - 1)(X^3 + X^2 + 1) = X^4 + X^2 + X + 1$.
- *Le code* C_7 *engendré par* $g_7(X) = (X^3 + X + 1)(X^3 + X^2 + 1) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.
- *Le code* C_8 *engendré par* $g_8(X) = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1) = X^7 - 1$.

$$C = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\}$$

Soit le code C_4 *engendré par* $g_4(X) = X^3 + X^2 + 1$, *a pour polynôme de contrôle:*

$$h_4(X) = \frac{X^7 - 1}{g_4(X)} = X^4 + X^3 + X^2 + 1 = g_5(X).$$

Une matrice génératrice G *et une matrice de contrôle* H *sont donc:*

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \; H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

3.4 Calcul de la distance minimum des codes cycliques $[n, n/2]$ sur GF(7)

3.4.1 Codes cycliques optimaux $[n, n/2]$ sur GF(7)

Soit le corps fini de **Galois** à 7 éléments noté $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, un code $C[n, k]_7$ linéaire est un sous espace vectoriel de dimension k sur $\mathbb{F}_7^n$.

Les éléments de C sont appelés mots de code et le poids $wt(x)$ d'un mot de code x est le nombre de positions où x différent de zéro.

La distance de **Hamming** $d(x, y)$ entre deux mots de codes est définie par:

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

La distance minimal d'un code linéaire C est :

$$d(C) = \min\{d(x, y)/x, y \in C, x \neq y\}.$$

Si C un code linéaire alors d(C) est égale au poids minimum de tous ses mots de code non nuls.

Le probleme fondamentale de la théorie du codage est:

trouver $d_q(n, k)$, la plus grande valeur de d pour laquelle un code $C[n, k, d]_q$ existe, un code qui atteint cette valeur est appelé un code **optimal**.

En utilisant l'algorithme de **Chen**, tel qu'il est décrit dans l'article:

José Felipe Voloch, "Computing the minimal distance of cyclic codes",computational & applied Mathematics, vol. 24, n°3, pp 393-398, 2005.

Notre recherche est axée sur l'optimisation de la distance minimale des codes cycliques $C[n, n/2]_7$, où n est pair non multiple de 7 et inférieur ou égale à 50.

Code cyclique de paramètres $C[2, 1]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^2 - 1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1.

$$X^2 - 1 = (1 + X)(6 + X).$$

On enregistre dans la table 1 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 1

n°	$g(X)$	mot de code (a)	$wt(a)$
1	11	11	**2**
2	61	61	**2**

Proposition 3.4.1 *La distance minimale optimale des codes cycliques* $C[2,1]_7$, *est* $d_C(2) = 2$.

Code cyclique de paramètres $C[4,2]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^4 - 1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et un polynôme de degré 2.

$$X^4 - 1 = (1 + X)(6 + X)(1 + X^2)$$

On enregistre dans la table 2 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 2

n°	$g(X)$	mot de code (a)	$wt(a)$
1	601	1060	**2**
2	101	1010	**2**

Proposition 3.4.2 *La distance minimale optimale des codes cycliques* $C[4,2]_7$, *est* $d_C(4) = 2$.

Code cyclique de paramètres $C[6,3]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^6 - 1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1.

$$X^6 - 1 = (1 + X)(2 + X)(3 + X)(4 + X)(5 + X)(6 + X).$$

Ainsi pour avoir un polynôme générateur de degré 3, il faut choisir 3 polynômes parmi les 6 de degré 1, ce qui donne: $\binom{6}{3} = 20$.

Donc il existe 20 polynômes générateurs de degré 3.

On enregistre dans la table 3 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 3

n°	$g(X)$	mot de code (a)	$wt(a)$
1	6461	310061	**4**
2	1001	100100	2
3	3311	010204	3
4	5621	010204	3
5	5511	010402	3
6	1221	110660	**4**
7	4631	010402	3
8	6131	110502	**4**
9	3641	010402	3
10	2651	010204	3
11	3521	010101	3
12	2331	010101	3
13	1141	110014	**4**
14	5341	010101	3
15	6251	210301	**4**
16	4361	010204	3
17	4551	010101	3
18	2561	010402	3
19	6001	100600	2
20	1411	210560	**4**

Proposition 3.4.3 *La distance minimale optimale des codes cycliques* $C[6, 3]_7$, *est* $d_C(6) = 4$.

Remarque 3.4.1 *Il ya exactement 6 codes cycliques optimaux $C[6,3]_7$ parmi les 20 codes cycliques existents.*

Code cyclique de paramètres $C[8,4]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme X^8-1 en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 3 polynômes de degré 2.

$$X^8-1=(1+X)(6+X)(1+X^2)(1+3X+X^2)(1+4X+X^2).$$

Ainsi pour avoir un polynôme générateur de degré 4, il faut choisir 2 polynômes parmi les 6 de degré 1 et en choisir un polynôme de degré 2 ou choisir 2 polynômes parmi les 3 de degré 2, ce qui donne:

$$\binom{2}{2}\times\binom{3}{1}+\binom{3}{2}=6.$$

Donc il existe 6 polynômes générateurs de degré 4.

On enregistre dans la table 4 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 4

n°	$g(X)$	mot de code (a)	wt(a)
1	60001	10006000	2
2	64031	31000640	**4**
3	63041	41000630	**4**
4	13231	51002001	**4**
5	14241	21002001	**4**
6	10001	10001000	2

Proposition 3.4.4 *La distance minimale optimale des codes cycliques $C[8,4]_7$,*

est $d_C(8)=4$.

Remarque 3.4.2 *Il ya exactement 4 codes cycliques optimaux $C[8,4]_7$ parmi les 6 codes cycliques existents.*

Code cyclique de paramètres $C[10, 5]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{10}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 2 polynômes de degré 4.

$$X^{10} - 1 = (1 + X)(6 + X)(1 + X + X^2 + X^3 + X^4)(1 + 6X + X^2 + 6X^3 + X^4).$$

Ainsi pour avoir un polynôme générateur de degré 5, il faut choisir un polynôme parmi les 2 polynômes de degré 1 et en choisir un polynôme de degré 4 , ce qui donne:

$$\binom{2}{1} \times \binom{2}{1} = 4.$$

Donc, il existe 4 polynômes générateurs de degré 5.

On enregistre dans la table 5 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 5

n°	$g(X)$	mot de code (a)	wt(a)
1	122221	1100066000	**4**
2	100001	1000010000	2
3	600001	1000060000	2
4	625251	6100061000	**4**

Proposition 3.4.5 *La distance minimale optimale des codes cycliques* $C[10, 5]_7$, *est* $d_C(10) = 4$.

Remarque 3.4.3 *Il ya exactement 2 codes cycliques optimaux* $C[10, 5]_7$ *parmi les 4 codes cycliques existents.*

Code cyclique de paramètres $C[12, 6]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{12}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1 et 3 polynômes de degré 2.

$$X^{12} - 1 = (1 + X)(2 + X)(3 + X)(4 + X)(5 + X)(6 + X)(1 + X^2)(2 + X^2)(4 + X^2).$$

Ainsi pour avoir un polynôme générateur de degré 6, ce qui nous donne:

$$\binom{6}{6} + \binom{3}{3} + \binom{6}{2} \times \binom{3}{2} + \binom{6}{4} \times \binom{3}{1} = 92.$$

Donc, il existe 92 polynômes générateurs de degré 6.

On choisir deux polynômes générateurs de degré 6, et on enregistre dans la table 6 les résultats de calcul des poids des mots de codes:

Table 6

n°	$g(X)$	mot de code (a)	wt(a)
1	4115541	600100600100	4
2	5436431	201000506000	4
...	...	...	...

Proposition 3.4.6 *La distance minimale optimale des codes cycliques* $C[12, 6]_7$, *est* $d_C(12) \geq 4$.

Code cyclique de paramètres $C[16, 8]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{16}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 7 polynômes de degré 2.

$$\begin{aligned} X^{16} - 1 &= (1+X)(6+X)(1+X^2)(6+X+X^2)(1+3X+X^2)(6+3X+X^2) \\ &\quad (1+4X+X^2)(6+4X+X^2)(6+6X+X^2). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 8, ce qui nous donne:

$$\binom{2}{2} \times \binom{7}{3} + \binom{7}{4} = 70.$$

Donc, il existe 70 polynômes générateurs de degré 8.

On choisir deux polynômes générateurs de degré 8, et on enregistre dans la table 7 les résultats de calcul des poids des mots de codes:

Table 7

n°	$g(X)$	mot de code (a)	wt(a)
1	124355341	6610000011600000	6
2	620224631	1000100010001000	4
...	...	...	...

Proposition 3.4.7 *La distance minimale optimale des codes cycliques* $C[16, 8]_7$, *est* $d_C(16) \geq 6$.

Code cyclique de paramétres $C[18, 9]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{18}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1 et 4 polynômes de degré 3.

$$X^{18}-1 = (1+X)(2+X)(3+X)(4+X)(5+X)(6+X)(2+X^3)(3+X^3)(4+X^3)(5+X^3).$$

Ainsi pour avoir un polynôme générateur de degré 9, ce qui nous donne:

$$\binom{6}{6} \times \binom{4}{1} + \binom{6}{3} \times \binom{4}{2} + \binom{4}{3} = 128.$$

Donc, il existe 128 polynômes générateurs de degré 9.

On choisir deux polynômes générateurs de degré 9, et on enregistre dans la table 8 les résultats de calcul des poids des mots de codes:

Table 8

n°	$g(X)$	mot de code (a)	wt(a)
1	6364656411	200100000100500500	5
2	1314151411	300600001000060121	7
...	...	...	...

Proposition 3.4.8 *La distance minimale optimale des codes cycliques* $C[18, 9]_7$, *est* $d_C(18) \geq 7$.

Code cyclique de paramètres $C[20, 10]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{20}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et un polynôme de degré 2 et 4 polynômes de degré 4 .

$$\begin{aligned} X^{20}-1 &= (1+X)(6+X)(1+X^2)(1+X+X^2+X^3+X^4)(1+4X+4X^2+3X^3+X^4) \\ &\quad (1+3X+4X^2+4X^3+X^4)(1+6X+X^2+6X^3+X^4). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 10, ce qui nous donne:

$$\binom{2}{2} \times \binom{4}{2} + \binom{1}{1} \times \binom{4}{2} = 12.$$

Donc, il existe 12 polynômes générateurs de degré 10.

On enregistre dans la table 9 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 9

n°	$g(X)$	mot de code (a)	wt(a)
1	62603051041	10300100000004050430	**7**
2	63062040151	10301000000020060206	**7**
3	60000000001	10000000006000000000	2
4	60205020501	60100000006010000000	4
5	64012040121	10301000000020010501	**7**
6	65603056031	60400100000004050440	**7**
7	15331302241	60000100006000010000	4
8	14220313351	60000100006000010000	4
9	10202020201	10100000006060000000	4
10	10000000001	10000000001000000000	2
11	13250414321	10000100001000010000	4
12	12341405231	10000100001000010000	4

Proposition 3.4.9 *La distance minimale optimale des codes cycliques* $C[20, 10]_7$, *est* $d_C(20) = 7$.

Remarque 3.4.4 *Il ya exactement 4 codes cycliques optimaux* $C[20, 10]_7$ *parmi les 12 codes cycliques existents.*

Code cyclique de paramétres $C[22, 11]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{22}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 2 polynômes de degré 10 .

$$\begin{aligned} X^{22}-1 &= (1+X)(6+X)(1+X+X^2+X^3+X^4+X^5+X^6+X^7+X^8+X^9+X^{10}) \\ &\quad (1+6X+X^2+6X^3+X^4+6X^5+X^6+6X^7+X^8+6X^9+X^{10}). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 11, ce qui nous donne:

$$\binom{2}{1} \times \binom{2}{1} = 4.$$

Donc, il existe 4 polynômes générateurs de degré 11.

On enregistre dans la table 10 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 10

n°	$g(X)$	mot de code (a)	wt(a)
1	12222222221	1100000000660000000000	**4**
2	10000000001	1000000000001000000000	2
3	60000000001	1000000000006000000000	2
4	65255255251	6100000000006100000000	**4**

Proposition 3.4.10 *La distance minimale optimale des codes cycliques* $C[22, 11]_7$, *est* $d_C(22) = 4$.

Remarque 3.4.5 *Il ya exactement 2 codes cycliques optimaux* $C[22, 11]_7$ *parmi les 4 codes cycliques existents.*

Code cyclique de paramètres $C[24, 12]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{24}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1 et 9 polynômes de degré 2.

$$\begin{aligned} X^{24}-1 &= (1+X)(2+X)(3+X)(4+X)(5+X)(6+X)(1+X^2)(2+X^2)(4+X^2)(4+X+X^2) \\ &\quad (2+2X+X^2)(1+3X+X^2)(1+4X+X^2)(2+5X+X^2)(4+6X+X^2). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 12, ce qui nous donne :

$$\binom{6}{6} \times \binom{9}{3} + \binom{6}{4} \times \binom{9}{4} + \binom{6}{2} \times \binom{9}{5} + \binom{9}{6} = 3948.$$

Donc, il existe 3948 polynômes générateurs de degré 12.

On choisir deux polynômes générateurs de degré 12, et on enregistre dans la table 11 les résultats de calcul des poids des mots de codes:

Table 11

n°	$g(X)$	mot de code (a)	wt(a)
1	5046046046041	40010.....0300060..0	4
2	4015203160231	60010.....060010....0	4
...	...	...	...

Proposition 3.4.11 *La distance minimale optimale des codes cycliques* $C[24, 12]_7$, *est* $d_C(24) \geq 4$.

Code cyclique de paramètres $C[26, 13]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{26}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 2 polynômes de degré 12.

$$\begin{aligned} X^{26}-1 &= (1+X)(6+X)(1+X+X^2+X^3+X^4+X^5+X^6+X^7+X^9+X^{10}+X^{11}+X^{12}) \\ &\quad (1+6X+X^2+6X^3+X^4+6X^5+X^8+X^6+6X^7+X^8+6X^9+X^{10}+6X^{11}+X^{12}). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 13, ce qui nous donne :

$$\binom{2}{1} \times \binom{2}{1} = 4$$

Donc, il existe 4 polynômes générateurs de degré 13.

On enregistre dans la table 12 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 12

n°	$g(X)$	mot de code (a)	wt(a)
1	12222222222221	11000000000006600000000000	**4**
2	10000000000001	10000000000001000000000000	2
3	60000000000001	10000000000006000000000000	2
4	62525252525251	61000000000006100000000000	**4**

Proposition 3.4.12 *La distance minimale optimale des codes cycliques* $C[26, 13]_7$, *est* $d_C(26) = 4$.

Remarque 3.4.6 *Il ya exactement 2 codes cycliques optimaux* $C[26, 13]_7$ *parmi les 4 codes cycliques existents.*

Code cyclique de paramètres $C[30, 15]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{30}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1 et 6 polynômes de degré 4.

$$\begin{aligned} X^{30}-1 &= (1+X)(2+X)(3+X)(4+X)(5+X)(6+X)(1+X+X^2+X^3+X^4) \\ &\quad (2+X+4X^2+2X^3+X^4)(4+6X+2X^2+3X^3+X^4)(4+X+2X^2+4X^3+X^4) \\ &\quad (2+6X+4X^2+5X^3+X^4)(1+6X+X^2+6X^3+X^4). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 15, ce qui nous donne:

$$\binom{6}{3} \times \binom{6}{3} = 400.$$

Donc, il existe 400 polynômes générateurs de degré 15.

On choisir deux polynômes générateurs de degré 16, et on enregistre dans la table 13 les résultats de calcul des poids des mots de codes:

Table 13

n°	$g(X)$	mot de code (a)	wt(a)
1	4412401241136531	4000010...03000060.....0	4
2	3635664214456351	4000010...0200005000060000	5
...	...	...	...

Proposition 3.4.13 *La distance minimale optimale des codes cycliques* $C[30, 15]_7$, *est* $d_C(30) \geq 5$.

Code cyclique de paramètres $C[32, 16]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{32}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 7 polynômes de degré 2 et 4 polynômes de

degré 4.

$$\begin{aligned} X^{32}-1 &= (1+X)(6+X)(1+X^2)(6+X+X^2)(1+3X+X^2)(6+3X+X^2)(1+4X+X^2) \\ &\quad (6+4X+X^2)(6+6X+X^2)(6+X^2+X^4)(6+3X^2+X^4)(6+4X^2+X^4)(6+6X^2+X^4). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 16, ce qui nous donne:
$\binom{2}{2}\times\binom{7}{7}+\binom{2}{2}\times\binom{7}{1}\times\binom{4}{3}+\binom{2}{2}\times\binom{7}{3}\times\binom{4}{2}+\binom{2}{2}\times\binom{7}{5}\times\binom{4}{1}+$
$\binom{7}{2}\times\binom{4}{3}+\binom{7}{4}\times\binom{4}{2}+\binom{7}{6}\times\binom{4}{1}+\binom{4}{4}=646.$
Donc, il existe 646 polynômes générateurs de degré 16.

On choisir deux polynômes générateurs de degré 16, et on enregistre dans la table 14 les résultats de calcul des poids des mots de codes:

Table 14

n°	$g(X)$	mot de code (a)	wt(a)
1	16423651533043211	601010...0106060.....0	6
2	10666655442266111	140....0100000140..10..0	6
...	...	...	...

Proposition 3.4.14 *La distance minimale optimale des codes cycliques* $C[32,16]_7$, *est* $d_C(32)\geq 6$.

Code cyclique de paramètres $C[34,17]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{34}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 2 polynômes de degré 16.

$$\begin{aligned} X^{34}-1 &= (1+X)(6+X)(1+X+X^2+X^3+X^4+X^5+X^6+X^7+X^8+X^9+X^{10}+X^{11}+ \\ &\quad X^{12}+X^{13}+X^{14}+X^{15}+X^{16})(1+6X+X^2+6X^3+X^4+6X^5+X^6+6X^7+ \\ &\quad X^8+6X^9+X^{10}+6X^{11}+X^{12}+6X^{13}+X^{14}+6X^{15}+X^{16}) \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 17, ce qui nous donne: $\binom{2}{1}\times\binom{2}{1}=4$.
Donc, il existe 4 polynômes générateurs de degré 17.

On enregistre dans la table 15 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 15

n°	$g(X)$	mot de code (a)	wt(a)
1	122222222222222221	11000000000000000660000000000000000	**4**
2	100000000000000001	10000000000000000100000000000000000	2
3	600000000000000001	10000000000000000600000000000000000	2
4	625252525252525251	61000000000000000610000000000000000	**4**

Proposition 3.4.15 *La distance minimale optimale des codes cycliques* $C[34, 17]_7$, *est* $d_C(34) = 4$.

Remarque 3.4.7 *Il ya exactement 2 codes cycliques optimaux* $C[34, 17]_7$ *parmi les 4 codes cycliques existents.*

Code cyclique de paramètres $C[36, 18]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{36}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1 et 3 polynômes de degré 2 et 4 polynômes de degré 3 et 2 polynômes de degré 6.

$$\begin{aligned} X^{36}-1 &= (1+X)(2+X)(3+X)(4+X)(5+X)(6+X)(1+X^2)(2+X^2) \\ &\quad (4+X^2)(2+X^3)(3+X^3)(4+X^3)(5+X^3)(2+X^6)(4+X^6) \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 18, ce qui nous donne:

$\binom{6}{1}\times\binom{3}{1}\times\binom{4}{1}\times\binom{2}{2}+\binom{6}{1}\times\binom{3}{1}\times\binom{4}{3}\times\binom{2}{1}+\binom{6}{2}\times\binom{3}{2}\times\binom{4}{4}+\binom{6}{2}\times\binom{3}{2}\times\binom{2}{2}+\binom{6}{2}\times\binom{3}{2}\times\binom{4}{2}\times\binom{2}{1}+\binom{6}{3}\times\binom{4}{1}\times\binom{2}{2}+\binom{6}{3}\times\binom{3}{3}\times\binom{4}{3}+\binom{6}{3}\times\binom{3}{3}\times\binom{4}{1}\times\binom{2}{1}+\binom{6}{4}\times\binom{3}{1}\times\binom{4}{2}\times\binom{2}{1}+\binom{6}{4}\times\binom{3}{1}\times\binom{4}{4}+\binom{6}{4}\times\binom{3}{1}\times\binom{2}{2}+\binom{6}{5}\times\binom{3}{2}\times\binom{4}{1}\times\binom{2}{1}+\binom{6}{5}\times\binom{3}{2}\times\binom{4}{3}+\binom{6}{6}\times\binom{3}{3}\times\binom{4}{2}+\binom{6}{6}\times\binom{3}{3}\times\binom{2}{1}+\binom{6}{6}\times\binom{4}{4}+\binom{6}{6}\times\binom{2}{2}+\binom{6}{6}\times\binom{4}{2}\times\binom{2}{1}+\binom{4}{2}\times\binom{2}{2}+\binom{4}{4}\times\binom{2}{1}=2042.$

Donc, il existe 2042 polynômes générateurs de degré 18.

On choisir deux polynômes générateurs de degré 18, et on enregistre dans la table 16 les résultats de calcul des poids des mots de codes:

Table 16

n°	$g(X)$	mot de code (a)	wt(a)
1	6464231545623115461	0....010....040....0200000	3
2	3535123414531656411	20...010..010..050...50..0	5
...	...	...	...

Proposition 3.4.16 *La distance minimale optimale des codes cycliques* $C[36, 18]_7$, *est* $d_C(36) \geq 5$.

Code cyclique de paramètres $C[38, 19]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{38}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 12 polynômes de degré 3.

$$\begin{aligned} X^{38}-1 &= (1+X)(6+X)(1+2X+X^3)(6+2X+X^3)(1+3X+X^2+X^3) \\ &\quad (1+2X^2+X^3)(1+X+3X^2+X^3)(6+3X+3X^2+X^3) \\ &\quad (1+4X+3X^2+X^3)(6+X+4X^2+X^3)(1+3X+4X^2+X^3) \\ &\quad (6+4X+4X^2+X^3)(6+5X^2+X^3)(6+3X+6X^2+X^3). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 19, ce qui nous donne:

$$\binom{2}{1} \times \binom{12}{6} = 1848.$$

Donc, il existe 1848 polynômes générateurs de degré 19.

On choisir deux polynômes générateurs de degré 19, et on enregistre dans la table 17 les résultats de calcul des poids des mots de codes:

Table 17

n°	$g(X)$	mot de code (a)	wt(a)
1	12525214245236214031	1104000010...01104000010.....0	8
2	62142106335111364241	2012060....0010565010.....060	10
...	...	...	...

Proposition 3.4.17 *La distance minimale optimale des codes cycliques* $C[38, 19]_7$, *est* $d_C(38) \geq 10$.

Code cyclique de paramètres $C[40, 20]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{40}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 3 polynômes de degré 2 et 8 polynômes de degré 4.

$$\begin{aligned} X^{40}-1 &= (1+X)(6+X)(1+X^2)(1+3X+X^2)(1+4X+X^2)(1+X+X^2+X^3+X^4) \\ &\quad (1+3X+6X^2+X^3+X^4)(1+4X+4X^2+3X^3+X^4)(1+X+6X^2+3X^3+X^4) \\ &\quad (1+3X+4X^2+4X^3+X^4)(1+6X+6X^2+4X^3+X^4)(1+6X+X^2+6X^3+X^4) \\ &\quad (1+4X+6X^2+6X^3+X^4). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 20, ce qui nous donne:

$$\binom{2}{2}\times\binom{3}{3}\times\binom{8}{3}+\binom{2}{2}\times\binom{3}{1}\times\binom{8}{4}+\binom{3}{2}\times\binom{8}{4}+\binom{8}{5}=532.$$

Donc, il existe 532 polynômes générateurs de degré 20.

On choisir deux polynômes générateurs de degré 20, et on enregistre dans la table 18 les résultats de calcul des poids des mots de codes:

Table 18

n°	$g(X)$	mot de code (a)	wt(a)
1	6650334163523436254 51	6140...00210...0600040500300300	10
2	1663262323323111410 21	00010.....010.....01.....010.....0100	5
...	...	...	...

Proposition 3.4.18 *La distance minimale optimale des codes cycliques* $C[40, 20]_7$, *est* $d_C(40) \geq 10$.

Code cyclique de paramétres $C[44, 22]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{44}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et un polynômes de degré 2 et 4 polynômes

de degré 10.

$$\begin{aligned} X^{44}-1 &= (1+X)(6+X)(1+X^2)(1+X+X^2+X^3+X^4+X^5+X^6+X^7+X^8+X^9+X^{10}) \\ &\quad (1+2X+5X^2+2X^3+6X^4+5X^5+6X^6+2X^7+5X^8+2X^9+X^{10}) \\ &\quad (1+5X+5X^2+5X^3+6X^4+2X^5+6X^6+5X^7+5X^8+5X^9+X^{10}) \\ &\quad (1+6X+X^2+6X^3+X^4+6X^5+X^6+6X^7+X^8+6X^9+X^{10}). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 22, ce qui nous donne:

$$\binom{2}{2} \times \binom{4}{2} + \binom{1}{1} \times \binom{4}{2} = 12.$$

Donc, il existe 12 polynômes générateurs de degré 22.

On enregistre dans la table 19 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 19

n°	$g(X)$	mot de code (a)	wt(a)
1	64006336004030014410031	6600....0110...06600....0110.....0	**8**
2	61443663441063341143361	6600....0110...06600....0110.....0	**8**
3	60000000000000000000001	1000....0000...01000....0000.....0	2
4	63006431004030064310041	6100....0610...06100....0610.....0	**8**
5	60205020502050205020501	6010....0000...06010....0000.....0	4
6	66433164431064331644311	6100....0610...06100....0610.....0	**8**
7	13263311521212511336231	6000....0100...06000....0100.....0	4
8	16515533032623033551561	6000....0100...06000....0100.....0	4
9	10202020202020202020201	1010....0000...06060....0000.....0	4
10	10000000000000000000001	1000....0000...01000....0000.....0	2
11	11565234042124043256511	1000....0100...01000....0100.....0	4
12	14213416551515561431241	1000....0100...01000....0100.....0	4

Proposition 3.4.19 *La distance minimale optimale des codes cycliques* $C[44, 22]_7$, *est* $d_C(44) = 8$.

Remarque 3.4.8 *Il ya exactement 4 codes cycliques optimaux* $C[44, 22]_7$ *parmi les 12 codes cycliques existents.*

Code cyclique de paramètres $C[46, 23]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{46}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 2 polynômes de degré 22.

$$\begin{aligned} X^{46}-1 &= (1+X)(6+X)(1+X+X^2+X^3+X^4+X^5+X^6+X^7+X^8+X^9+X^{10}+X^{11}+ \\ &\quad X^{12}+X^{13}+X^{14}+X^{15}+X^{16}+X^{17}+X^{18}+X^{19}+X^{20}+X^{21}+X^{22}) \\ &\quad (1+6X+X^2+6X^3+X^4+6X^5+X^6+6X^7+X^8+6X^9+X^{10}+6X^{11}+X^{12} \\ &\quad +6X^{13}+X^{14}+6X^{15}+X^{16}+6X^{17}+X^{18}+6X^{19}+X^{20}+6X^{21}+X^{22}). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 23, ce qui nous donne:

$$\binom{2}{1} \times \binom{2}{1} = 4.$$

Donc, il existe 4 polynômes générateurs de degré 23.

On enregistre dans la table 20 les résultats de calcul des poids des mots de codes pour certains polynômes générateurs:

Table 20

n°	$g(X)$	mot de code (a)	wt(a)
1	122222222222222222222221	110.....0660.....0	**4**
2	100000000000000000000001	100.....0100.....0	2
3	600000000000000000000001	100.....0600.....0	2
4	625252525252525252525251	610.....0610.....0	**4**

Proposition 3.4.20 *La distance minimale optimale des codes cycliques* $C[46, 23]_7$, *est* $d_C(46) = 4$.

Remarque 3.4.9 *Il ya exactement 2 codes cycliques optimaux* $C[46, 23]_7$ *parmi les 4 codes cycliques existents.*

Code cyclique de paramètres $C[48, 24]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{48}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 6 polynômes de degré 1 et 21 polynômes de degré 2.

$$\begin{aligned} X^{48}-1 &= (1+X)(2+X)(3+X)(4+X)(5+X)(6+X)(1+X^2)(2+X^2) \\ &\quad (4+X^2)(3+X+X^2)(4+X+X^2)(6+X+X^2)(2+2X+X^2) \\ &\quad (3+2X+X^2)(5+2X+X^2)(1+3X+X^2)(5+3X+X^2)(6+3X+X^2) \\ &\quad (1+4X+X^2)(5+4X+X^2)(6+4X+X^2)(2+5X+X^2)(3+5X+X^2) \\ &\quad (5+5X+X^2)(3+6X+X^2)(4+6X+X^2)(6+6X+X^2). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 24, ce qui nous donne:

$$\binom{6}{2}\times\binom{21}{11}+\binom{6}{4}\times\binom{21}{10}+\binom{6}{6}\times\binom{21}{9}+\binom{21}{12}=11\,169\,340.$$

Donc, il existe 11 169 340 polynômes générateurs de degré 24.

On choisir deux polynômes générateurs de degré 24, et on enregistre dans la table 21 les résultats de calcul des poids des mots de codes:

Table 21

n°	$g(X)$	mot de code (a)	wt(a)
1	362315402105315462305602 1	60030...010010...00600004000050000200	8
2	232645100151400251500045 1	10.....010.....010.....010.....0	4
...	...	...	...

Proposition 3.4.21 *La distance minimale optimale des codes cycliques* $C[48, 24]_7$, *est* $d_C(48) \geq 8$.

Code cyclique de paramètres $C[50, 25]_7$

En utilisant **Mathematica 9,** la factorisation du polynôme $X^{50}-1$ en facteurs irréductibles sur le corps $\mathbb{F}_7$ donne 2 polynômes de degré 1 et 12 polynômes de degré 4.

$$\begin{aligned} X^{50}-1 &= (1+X)(6+X)(1+X+X^2+X^3+X^4)(1+X+5X^2+X^3+X^4) \\ &\quad (1+2X+4X^2+2X^3+X^4)(1+2X+5X^2+2X^3+X^4) \\ &\quad (1+3X+3X^3+X^4)(1+3X+3X^2+3X^3+X^4)(1+4X+4X^3+X^4) \\ &\quad (1+4X+3X^2+4X^3+X^4)(1+5X+4X^2+5X^3+X^4) \\ &\quad (1+5X+5X^2+5X^3+X^4)(1+6X+X^2+6X^3+X^4)(1+6X+5X^2+6X^3+X^4). \end{aligned}$$

Ainsi pour avoir un polynôme générateur de degré 25, ce qui nous donne:

$$\binom{2}{1} \times \binom{12}{6} = 1848.$$

Donc, il existe 1848 polynômes générateurs de degré 25.

On choisir deux polynômes générateurs de degré 25, et on enregistre dans la table 22 les résultats de calcul des poids des mots de codes:

Table 22

n°	$g(X)$	mot de code (a)	wt(a)
1	621310560334343440120646 51	10..060..010..060..010..060..010..060..010..60..0	10
2	1113321605322223506123311 1	55060....020....050....01022010....050...020...060	12
...	...	...	...

Proposition 3.4.22 *La distance minimale optimale des codes cycliques* $C[50, 25]_7$, *est* $d_C(50) \geq 12$.

3.4.2 Le tableau de la distance minimum optimale des codes cycliques [n,n/2]$_7$

Pour n pair et $(2 \leq n \leq 50)$:

n	2	4	6	8	10	12	16	18	20	22	24
n/2	1	2	3	4	5	6	8	9	10	11	12
nbre de $g(X)$	2	2	20	6	4	92	70	128	12	4	3948
d_C	2	2	4	4	4	≥ 4	≥ 6	≥ 7	7	4	≥ 4

n	26	30	32	34	36	38	40	44	46	48	50
n/2	13	15	16	17	18	19	20	22	23	24	25
nbre de $g(X)$	4	400	646	4	2042	1848	532	12	4	11 169 340	1848
d_C	4	≥ 5	≥ 6	4	≥ 5	≥ 10	≥ 10	8	4	≥ 8	≥ 12

Conclusion

L'objectif principal de cette mémoire est cherché la meilleure distance minimale des codes cycliques optimaux de rendement 1/2 sur le corps fini à 7 éléments, jusqu'à un code de longueur 50, et de paramètres [n,n/2] sur F_7, pour n pair non multiple de 7.

Bibliographie

[1] **-A.Bonnecaze**.Cours introduction à l'algébre pour les codes cycliques. Université d'Aix-Marseille (2006-2007).

[2] **-Aicha Batoul**. Construction des codes auto-duaux. Thèse présentée pour l'obtention du diplôme de Doctorat, Université des Sciences et de la Technologie Houari Boumediene 2013.

[3] **-Alain Kraus.** Cours d'arithmétique. Université Pierre et Marie Curie 2012-2013.

[4] **-Bruno Deschamps.** Théorie de Galois, cours de maitrise. Université Saint-Etienne 2002-2003.

[5] **-Cherif Mihoubi.** Classification des codes linéaires tertiaires optimaux [n,n/2]. Thèse présentée pour l'obtention du diplôme de Doctorat, Université Hadj Lakhdar Batna 2012.

[6] **-Cherif Mihoubi.** Cours corps finis et polynômes. Université de M'sila 2014-2015.

[7] **-Cherif Mihoubi & Patrick Solé.** Optimal and isodual ternary cyclic codes of rate 1/2.Received : 12 January 2012 / Revised: 9 May 2012 / Accepted: 4 July 2012 / Published online: 26 July 2012 © The Author(s) 2012. This article is published with open access at SpringerLink.com.(343–357).

[8] **-Dany-Jack.** Corps finis, IUFM de Guadeloupe, Morne Ferret, BP399, Pointe-à-Pitre cedex 97159, dany-jack.mercier@univ-ag.fr, 11 avril 2003.

[9] **-Gilles Zémor.** Master CSI: Arithmétique corps finis et applications (11-12-2006).

[10] **-Haboub Lakhdar.** Etude de techniques de décodage des codes linéaires. Mémoire pour l'obtention du diplôme de Magistère. Université de M'sila 2009-2010.

[11] **-Hans Bherer.** Théorie algébrique du codage. Mémoire présenté à la Faculté des études supérieures, Université Laval pour l'obtention du grade de maîtrise Sciences (M.Sc), Septembre 2000.

[12] **-Jean-Jacques Risler et Pascal Boyer.** Algébre pour la licence 3, groupes, anneaux, corps, cours et exercices corrigés. Dunod, Paris, 2006.

[13] **-Nicolas Bruyere.** Eléments de théorie des corps finis. Application : les codes correcteurs. Université de Rouen, Agrégation de mathématiques 2005-2006.

[14] **-Odile Papini.** Introduction à la théorie des codes correcteurs d'erreurs (Codes cycliques). Polytech Université d'Aix-Marseille.

[15] -**Pierre Abbrugiati.** Introduction aux codes correcteurs d'erreurs (23 janvier 2006).

[16] **-Pierre Wassef.** Cours d'arithmétique LM 220. Université Pierre & Marie Curie.